Sicherheit im Internet

Hausarbeit

Leistungsschein

an der

BTU - COTTBUS

Lehrstuhl Betriebliche Bildung / Dipl.-Ing. Jost- Peter Kania

Studiengang: Umweltingenieurwesen und Verfahrenstechnik

Fachsemester 4

Seminar: „Didaktische Grundlagen nutzerfreundlicher Gestaltung von Angeboten im Internet - Analyse und Entwicklung von Webseiten“

Cottbus, Juni 2000

Inhaltsverzeichnis

1 Einleitung

Leider bietet das Internet nicht nur Vorteile, sondern es lauern auch sehr viele Gefahren im Netz. Immer öfter hört man von Angriffen auf Rechnersysteme. Das aktuelle Beispiel des E-Mail-Virus "I LOVE YOU" zeigt, dass es eine Vielzahl von Sicherheitslücken im Softwarebereich gibt, die innerhalb von Stunden weltweit zu Millionenschäden führten. Dabei richten sich die Internetangriffe nicht nur gegen Behörden oder Firmen. Jeder Internetuser kann von diesen Attacken betroffen sein.
Deshalb spielen Sicherheitskonzepte eine immer größere Rolle.
In unserem Vortrag werden wir auf einige Gefahren und Sicherheitssysteme hinweisen und sie erläutern. Dabei erläutern wir zuerst die Gefahr von Viren. Im nächsten Kapitel stellen wir die sogenannten Firewalls vor. Danach gehen wir auf Spamming und Cookies ein. Zum Thema Sicherheitsvorkehrungen stellen wir Kryptographie und PGP vor und zum Schluss erklären wir, auf welche Arten man im Internet bezahlen kann und wobei dort die Gefahren liegen.

2 Viren

2.1 Allgemeines

Laut Definition ist ein Computervirus eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.
Es existieren viele Arten von Viren, die sich in ihrer Verbreitung, ihren Auswirkungen und auch in ihrem Aussehen unterscheiden. Heute schätzt man ihre Zahl auf rund 46 000 Stück, täglich kommen rund 15 neue hinzu. In freier Wildbahn wird ihre Zahl aber auf unter 1 000 geschätzt.
In der Realität wurde der erste Virus 1986 auf IBM-PCs entdeckt. Seit diesem Zeitpunkt gibt es den Wettlauf zwischen Programmierern immer komplizierterer Viren und ihren Gegenspielern, den Entwicklern von Antivirensoftware.

2.2 Arten von Viren

Trotz der Vielzahl von Arten, kann man den Viren gemeinsame Hauptaufgaben zuweisen. Diese bestehen zum einen darin, das eigene Programm zu kopieren, um eine große Verbreitung zu erreichen, zum anderen das Zerstören von Daten durch Ausführung eines entsprechenden Programmteils. Ein Virus muss aber nicht unbedingt Schaden anrichten, er kann z.B. auch einfach nur am 24. Dezember Weihnachtsgrüße auf den Bildschirm bringen Heute unterscheidet man im wesentlichen 3 Arten der unerwünschten Programme: Bootsektor-, Datei- und die immer "beliebter" werdenden Makroviren.

2.3 Funktionsweise

Der Bootsektor-Virus ist bemüht, sich selbst anstelle der Grundroutinen einzusetzen und so noch vor dem Start der eigentlichen Systemprogramme aktiv zu werden. Er kopiert sich von selbst auf noch nicht befallene Datenträger. Ist dieses erfolgt, aktiviert er ein Unterprogramm, das dann zum Beispiel die Einträge der File Allocation Table (FAT) und damit die Daten der Festplatte löscht.

Die Hauptaufgabe des Dateivirus besteht darin Dateien bestimmter Typen zu befallen, vornehmlich ausführbare Programme oder Bibliotheksdateien. Sind solche Dateien befallen, wird bei einem Aufruf zuerst der Viruscode gestartet. Dieser verursacht den Befall weiterer Dateien. Dadurch kann je nach Ausführung des Virus entweder die ganze Dateistruktur der einen oder aller Dateien zerstört werden.

Active Content, die Möglichkeit zunächst passive Dokumente mit ausführbarem Code zu bereichern, ist die Grundlage des Makrovirus. Makros wie Word-, Excel- und Powerpoint werden beim Aufrufen eines Dokumentes ausgeführt und können sich dann in gleichartigen Dateien oder auch solchen einer anderen Anwendung einnisten. Dadurch, dass Dokumente viel häufiger verschickt werden als Programme ist die Verbreitung rasant. Dazu kommt auch, dass Makros systemübergreifend lauffähig sind, wodurch beispielsweise ein Virus von Windows auf den Mac übertragen werden kann. 1996 wurden noch 83% aller Schäden durch Bootsektorviren verursacht , 1999 war in 64% aller Fälle ein Makrovirus verantwortlich.

Neben den beschriebenen drei Hauptgruppen, gibt es auch Mischformen. Eine wichtige Mischformen sind polymorphe Viren. Sie sind in der Lage, sich nicht nur zu vermehren sondern auch zu verändern.

2.4 Trojanische Pferde

"Trojanische Pferde" sind streng genommen keine Viren, da sie eigenständige Programme darstellen, sich aber nicht vermehren, tun sie es doch, nennt man sie Würmer.
Der Typ "Hoax" ist auch kein Virus sondern eine meist per E-Mail versandte dramatische Warnung vor einem vermeintlichen Übel, die man an möglichst viele Empfänger weiterleiten sollte. Der einzige Schaden ist unnötige Aufregung und verlorene Arbeitszeit.

2.5 Bekämpfung von Viren

Bei der Bekämpfung der Viren durch Antivirenprogramme spielen Polymorphe und Makroviren ein wichtige Rolle. Da der polymorphe Virus in der Lage ist, sich selbst zu verändern, und trotzdem seine Aufgabe wahrzunehmen, ist der Virus für herkömmliche Virenscanner schlecht zu erkennen. Denn diese suchen nach sogenannten Signaturen, die typisch für ein einmal erkanntes Virus sind, bei Veränderung des Virus ändert sich auch seine Signatur.
Neben der Virensuche durch Signaturanalyse gibt es auch die heuristische Virensuche. Bei dieser Methode wird versucht, das Verhaltensmuster eines Programms nachzuvollziehen, und bei kritischen Befehlen (Dateien löschen, formatieren) Alarm zu geben. Die heuristische Virensuche allein führt zur Erkennung von 70-80%, zusammen mit der Signaturanalyse beträgt die Trefferquote über 95%. Bei der Auswahl eines geeigneten Antiviren-Programms gibt es mehrere Punkte zu beachten. Es sollte folgendes können:

- vollständige Untersuchung des Bootsektors der Startfestplatte sowie aller Datenträgersysteme
- Überprüfung aller auf den Datenträgern enthaltenen Dateien
- Überprüfung von E-Mail -Attachments auf spezielle Viren oder befallene Dateien
- Aktuelle Virusdefinition nach Möglichkeit per Internet-Update
- Überprüfen von Archivdateien (ZIP,RAR)
- Überprüfen von Download –Dateien

Doch ein gutes Antiviren-Programm allein ist keine Garantie. Man sollte zur Sicherheit auch einige grundsätzliche Verhaltensregeln beachten. Ein moderner "Virenkiller" sollte eines der ersten Programme sein, welches man auf seinem Rechner installiert. Denn nur so kann man sicher sein, dass alle nachfolgenden Installationen automatisch überwacht werden.

Auch sollte man sich nur Programme bekannter Download-Pools herunterladen, da große Anbieter ihre Daten ständig auf Viren prüfen.
Des weiteren sollte man keine Programme unbekannter Herkunft installieren, denn die meisten Viren werden durch Raubkopien verbreitet. Wichtig ist auch, dass sich beim Booten keine Disketten im Laufwerk befinden, da viele Rechner so eingestellt sind, dass sie als erstes das Disketten -Laufwerk abfragen. Ist die entsprechende Diskette verseucht, wird sie beim Bootvorgang aktiviert. Große Vorsicht ist bei E-Mail -Attachments geboten, besonders wenn die Quelle nicht bekannt ist. E-Mails mit Anhang -Dateien können leicht Viren enthalten. Deshalb sollte man Antivirenprogramme benutzen, die auch E -Mails und Attachements untersuchen. Nicht zuletzt ist es ratsam, sich im Bezug auf aktuelle Viren und deren Erkennung ständig auf dem laufenden zu halten. Wissen und Information sind fast immer schon die halbe Miete, wenn es darum geht sich erfolgreich vor Viren zu schützen.

3 Firewalls

3.1 Allgemeines

Zur Einleitung ist hier folgendes Beispiel angebracht.
Am 30. Dezember 1996 gelang es einem Hacker eine Seite der U.S. Air Force mit Statistiken durch ein pornographisches Bild zu ersetzen. Die Air Force wurde erst durch Anfragen der Presse, die anonym verständigt worden war, auf diesen Vorfall aufmerksam, der Server musste für mehr als 24 Stunden vom Netz genommen werden.
In den letzten Jahren wurde die weltweite Vernetzung von Computern schnell vorangetrieben. Dadurch erhöhten sich auch die Sicherheitsrisiken. Bei den nur lokal vernetzten Systemen (LANs) ist ein Einbruch erst nach dem Vordringen zu einem Rechner des LANs möglich.
Die Sicherheit basiert dabei im wesentlichen auf physikalischen und personellen Sicherheitsmaßnahmen (z.B. Türen, Zäunen oder Pförtnern). Durch die Anbindung an Weiterverkehrsnetze wie dem Internet werden diese Sicherheitsmaßnahmen leicht umgehbar. Alle Rechner des LANs sind weltweit erreichbar und damit angreifbar. Da viele Dienste nur über schwache Sicherungsmaßnahmen verfügen (NFS, NIS, TFTP, rlogin) und zudem in vielen Servern katastrophale Fehler enthalten sind, ist bei den meisten Rechnern ein Eindringen für einen Angreifer problemlos möglich.

Warum werden die Rechner überhaupt angegriffen? Hacker, die ertappt wurden, gaben hauptsächlich folgende Motive an: Sie suchten die technische Herausforderung und wollten ihren Ehrgeiz stillen, bei anderen handelte es sich um entlassene Angestellte, die sich an ihrer Firma rächen wollten und vielen ging es dabei natürlich auch um das Geld (Stichwort: Industriespionage).
Praktisch kann jeder Server am Internet das Ziel eines Angriffes werden, auch wenn es dort eigentlich nichts „zu holen“ gibt. Noch mehr gefährdet sind naturgemäß Server oder Netze, die bekannten Firmen oder Personen zugeordnet werden.
Die Rechner können zwar so konfiguriert werden, dass sie weitgehend gegen Angriffe aus dem Netz gesichert sind, aber dafür muss auf viele angenehme und nützliche Dienste verzichtet werden. Außerdem ist es notwendig, alle Rechner des LANs gleichermaßen zu schützen, da ein Angreifer sonst über den am schwächsten gesicherten Rechner ins LAN eindringt. Bei großen LANs ist eine Absicherung aller Rechner jedoch kaum möglich.

3.2 Der Begriff Firewall

Zur Absicherung von LANs gegen Angriffe von außen werden in letzter Zeit häufig Firewalls eingesetzt. Der Firewall stellt nach außen hin nur eine kleine Anzahl gut gesicherter und streng überwachter Dienste zur Verfügung. Jede Kommunikation der Rechner im LAN untereinander wird durch diesen Sicherheitsmechanismus nicht beeinträchtigt.
Der Begriff „Firewall“ kommt aus der Architektur und kann mit „Brandschutzmauer“ übersetzt werden. Brandschutzmauern sollen die Ausbreitung eines Feuers stoppen oder es zumindest, solange aufhalten bis Hilfe eintrifft. Die Aufgabe eines Firewalls bei Netzwerken ist ähnlich, geht jedoch über das Stoppen oder Aufhalten von Angriffen hinaus. Für einen Firewall kann man folgende Definition formulieren: „Ein Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Es wird dafür gesorgt, dass jede Kommunikation zwischen den beiden Netzen über den Firewall geführt werden muss. Auf dem Firewall sorgen Zugriffskontrolle und Audit dafür, dass das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt werden.“

Ein Firewall dient also dazu, ein internes Netzwerk mit einem öffentlichen Netzwerk zu verbinden, von dem man annehmen muss, dass es potentielle Angreifer beherbergt. In den meisten Fällen werden sie eingesetzt, um ein lokales Netzwerk (LAN) gegen Angriffe aus dem Internet zu schützen. Dabei sollen den internen Nutzern die Vorteile des Internets zugänglich gemacht werden, ohne dabei Unbefugten Zugriff auf interne Daten zu bieten. Da jede Kommunikation zwischen den beiden Netzen über den Firewall geführt werden muss, ermöglicht dieser die Durchsetzung einer Sicherheitspolitik. Das Ziel ist es, Angriffe vom Internet zu verhindern und dabei die Benutzer des LANs sowenig, wie möglich zu behindern.

3.3 Bedarfsanalyse

Eine Organisation will also am Internet präsent sein. Es wäre nun relativ einfach, das bereits vorhandene lokale Netz mit offiziellen IP – Adressen auszustatten und über einen Router mit dem ISP zu verbinden. Dass dieser, häufig praktizierte, Ansatz der Keim für Katastrophen bis hin zur völligen wirtschaftlichen Vernichtung der Firma birgt, wird oft erst bemerkt, wenn der Schaden bereits entstanden ist. Genauso wie nicht alle Firmendaten in der Zeitung veröffentlicht werden, müssen auch vor dem Netzanschluss zumindest die folgenden Punkte abgeklärt werden: 1. Wie passen diese Anforderungen in das gesamte Sicherheitskonzept der Firma? 2. Genügt für diese Anbindung ein Datenserver, oder muss wirklich das gesamte Internet erreichbar sein? 3. Welche Mitarbeiter sollen welche Netzwerkfunktionen in welchem Umfang nutzen?

Oft wird in der anfänglichen Internet – Euphorie übersehen, dass z.B. die Möglichkeit, im Web zu surfen zwar viel Arbeitszeit kosten kann, aber nicht wirklich für alle Mitarbeiter zur Bewältigung der täglich gestellten Aufgaben notwendig ist. Es geht also um ein Gesamtsicherheitskonzept, in dem der Firewall nur einen wichtigen Teil darstellt.

Welche Sicherheit bietet ein Firewall? Einerseits ist ein Firewall ein Fokus für Sicherheitsentscheidungen. Die Installation eines Firewall macht es nötig klare Richtlinien für die Sicherheit in einem Computernetzwerk zu definieren. Damit wird vermieden, dass nur ein unscharfer Sicherheitsbegriff besteht, der dazu führt, dass bei konkreten Problemen stets ad-hoc Entscheidungen getroffen werden, die dann leicht untereinander inkonsistent sind. Andererseits ist ein Firewall ein zentraler Verbindungsknoten. Alle Daten die zwischen internem und externem Netz ausgetauscht werden, müssen durch den Firewall. Damit ist es möglich in dem Firewall die Durchsetzung der Sicherheitspolitik zu erzwingen, bzw.

Verstöße gegen Sicherheitsrichtlinien zu erkennen und zu protokollieren. Außerdem begrenzt ein Firewall die Angriffsfläche.

Ein externer Angreifer muss zunächst den Firewall überwinden, bevor er einen der internen Rechner attackieren kann. Da der Firewall eine, im Verhältnis zu einem großen, internen Netzwerk, kleine und daher überschaubare Einheit darstellt, ist eine gute Verteidigung des Firewall relativ einfach und erfolgsversprechend. Das bedeutet natürlich nicht, dass man völlig auf eine rechnergestützte Verteidigung im internen Netz verzichten kann, aber ein Angreifer sollte stets von dem Firewall abgefangen werden und keine Möglichkeit haben, die Stärken und Schwächen der internen Verteidigung zu erforschen.

3.4 Nachteile von Firewalls

Es gibt aber auch Dinge, vor denen ein Firewall kein Schutz bietet. Er schützt nicht vor Angriffen die innerhalb des lokalen Netzes vor sich gehen (etwa durch Personen, die physischen Zugang zu dem angegriffenen Computer haben). Ein Firewall kann auch nur jene Datenpakete untersuchen, die durch ihn geschickt werden. Wenn neben der offiziellen, durch den Firewall überwachten, Verbindung noch andere existieren (etwa privat installierte Modems innerhalb des internen Netzes), so kann der Firewall natürlich nicht überprüfen, welche Daten dort über die Leitung wandern. Insbesondere besteht dann die Gefahr, dass der Firewall von innen heraus angegriffen wird, und so über die Hintertür der Hauptzugang geöffnet wird. Ein Firewall verfügt über kein Verständnis für den Inhalt der Daten, die durch ihn fließen. Es gibt zu viele Protokolle, Kompressionsverfahren und Computertypen um automatisch sicher zu erkennen wann ein Datenpaket Teil eines Programms ist um dann einen Virenscanner zu starten.

3.5 Arten von Firewalls

Firewalls können grob nach ihrer Funktionsweise eingeteilt werden. Moderne Installationen vereinigen meistens mehrere der angeführten Funktionen.

Es gibt Firewalls auf Netzwerkebene, die sogenannten Paketfilter. Paketfilter sind relativ simple Teile und repräsentieren den ursprünglichen Firewall. Sie prüfen den Netzwerkverkehr nach festen Regeln, die vorher entsprechend dem Gesamtsicherheitskonzept aufgestellt wurden.

Der Inhalt der einzelnen Pakete wird ignoriert, nur allgemeine Daten wie Absender, Empfänger und Servicetyp können für Filterentscheidungen herangezogen werden. Die drei Arten der Paketfilter sind das Smart-Bridge, der Router und die IP-Maskerade.
Firewalls auf Applikationsebene führen die vom Benutzer gewünschte Funktion (z.B. Holen einer HTML – Seite) für diesen aus und stellen ihm danach das Ergebnis zur Verfügung. Dabei können die Benutzerwünsche auf ihre Konformität mit dem Sicherheitskonzept und die gewonnenen Daten einer Überprüfung unterzogen werden. Hierbei unterscheidet man Proxy – Server und Gateways.

4 Spam

Eine zwar nicht so gefährliche aber sicherlich unangenehme Sache ist das Spamming. Unter Spam wird eine E-Mail verstanden, die Werbung enthält und ohne Verlangen oder Zustimmung des Empfängers an diesen versandt wurde.
Werden solche E-Mails zugleich an eine Vielzahl von Empfängern gesendet, wird von Spamming gesprochen. Der Versender solcher Werbebotschaften wird als Spamer bezeichnet.
Diese im Internet verbreitete Begriffsbildung geht auf ein in England und den USA verbreitetes Dosenfleisch zurück, welches unter der Marke Spam angeboten wird. Spam stand ursprünglich für „spiced pork and ham“, ein Produkt der Firma Hormel Foods Corp., USA. Dieses Dosenfleisch spielt in einigen Sketchen der bekannten Komiker-Gruppe Monty Python eine Rolle. In einer Szene sang eine Gruppe Wikinger „Spam, Spam, Spam,...“, und unterdrückte damit jegliche Unterhaltung im Raum. Ein ähnlicher Effekt wird durch massenhaft versandte Werbung per E-Mail befürchtet, durch die Unmenge an Post können die Mailserver im Internet vollkommen überlastet werden und die wichtigen Nachrichten ihre Empfänger nur mit Mühe erreichen, da die privaten Postfächer der Internet-Nutzer durch Werbemüll versperrt werden. Das Spamming, also die massenweise Versendung von Werbung per E-Mail, ist für Werbetreibende attraktiv, da so eine große Anzahl Empfängern (nahezu) kostenlos erreichbar ist. Die Empfänger von unverlangt zugesandten Werbe-Mails sind dagegen meist alles andere als erbaut. Ihr Briefkasten wird verstopft und das Aussortieren von Werbung aus den „richtigen“ Mails ist lästig und zeitintensiv. Außerdem steigen durch die Zustellung der E-Mails mit der Werbung die Online-Zeiten und damit die Kosten.

Bei Spamming lässt also der Werbende seine Werbung durch den Beworbenen und die gesamte Internet-Gemeinschaft bezahlen. Daher wird Spamming von seriösen Unternehmen so gut wie nie angewandt.
Aber die Internet-User wehren sich. Sowohl politisch, als auch technisch wird versucht, Spammer in Schach zu halten. Bei der Europäischen Union in Brüssel werden Gesetze angestrengt unerwünschte kommerzielle E-Post zu reglementieren. Technisch versuchen Cityweb und andere Provider, durch Mail-Filter der Werbeschwemme Herr zu werden.

5 Cookies

Ein gewisses Sicherheitsrisiko stellen die sogenannten Cookies dar.
Cookies sind Informationen im ASCII-Format, die durch cgi oder JavaScript generiert werden, wenn man auf eine entsprechende Seite surft und dem Browser zum Ablegen auf der lokalen Platte übergeben werden. In ihnen werden verschiedene Informationen, die während einer Online Sitzung gesammelt wurden, abgelegt. Ein Cookie kann nur das tun, was der Browser zulässt. Und das ist bei modernen Browsern relativ wenig. Es können nämlich nur die Dinge abgefragt werden, die von dem Browser in den speziell für Cookies reservierten Bereich hineingeschrieben worden sind (bei Netscape ist das die Datei *cookies.txt*, beim Microsoft Internet Explorer das Verzeichnis *\cookies*). Nach den Definitionen dürfen pro Server außerdem nicht mehr als 20 Cookies abgelegt werden, insgesamt maximal 300 mit maximal 4 MB. Cookies sind also Informationen, die zuvor auf der Festplatte abgelegt worden sind und nur an den Server zurückgesandt werden, der sie damals gesetzt hatte.
Aber warum setzt man Cookies ein? Zum einem gibt es WebCounter, die durch Cookies die Zugriffe zählen; Bannerexchange Dienste, die sich damit die Anzahl der gezeigten Banner merken; getätigte Einkäufe werden gespeichert und man kann Webangebote personalisieren. Warum sollte jemand ein web Angebot personalisieren? Klare Antwort, um es den Surfern einfacher zu machen!
Nehmen wir an, man surft immer wieder auf eine Seite die zig Informationen anbietet. Jedes mal muss man sich durch eine Wust von Seiten klicken (die Gebühren laufen dabei mit) bis man zu der Rubrik kommt, die einen interessiert. Mit Hilfe der Cookies sucht man sich seine gewünschten Rubriken aus und lässt diese Informationen in einem Cookie auf die Festplatte legen. Wenn man wieder einmal zu Besuch kommt, dann wird man sofort, ohne langen Umweg, zu den Informationen geführt. Man spart somit wertvolle Online Zeit.

Aber warum kann es gefährlich sein Cookies einzusetzen? Dabei sei zunächst erwähnt, dass ein Cookie keine Viren übertragen, keine E-Mail Adressen und Platteninhalte auslesen kann. Es kann auch keine unbemerkten E-Mails versenden oder die gesamte Platte voll schreiben oder gar auslöschen. Im Zusammenhang mit Cookies spricht man oft vom „gläsernen Bürger“. Die Risiken beziehen sich meistens auf die Privatsphäre des Anwenders. Dadurch, dass ein Server sozusagen eine „Duftmarke“ auf der Platte hinterlässt und dieser (bekannte) Bereich von anderen Servern ausgelesen werden darf, kann man natürlich einiges über die Interessen, Vorlieben und Neigungen des Users erfahren – und zwar um so genauer, je mehr Cookies sich auf seiner Platte befinden.

Zwar können mit Hilfe der Cookies unsere Surfgewohnheiten protokolliert werden aber das bringt noch keine Gefahren mit sich. Erst wenn wir dann noch, bei einem Gewinnspiel zum Beispiel, unsere Identität lüften indem wir persönliche Daten per E-Mail versenden, entblößen wir uns. Wenn sich dann noch die Firmen zusammentun und die Daten austauschen, dann besteht die Möglichkeit, ein mehr oder weniger genaues Profil von einem zu bekommen.

Fragwürdig ist die Möglichkeit Nicknamen und Passwörter für irgendwelche Webpages per Cookies aufzunehmen. Denn man muss daran denken, dass die Cookies für jeden zugänglich sind der Zugang zum PC hat. Die Vorteile von Cookies ergeben sich beim „bestimmungsgemäßen“ Gebrauch. Das sind die Einsatzbereiche, für die die Cookies seinerzeit „erfunden“ wurden: Das Netz an die Bedürfnisse jedes einzelnen Anwenders anzupassen und ihm seine Arbeit zu erleichtern. Dazu gehört z.B. das Abspeichern von Passwörtern, so dass es nicht jedes mal eingegeben werden muss. Dabei sollte man aber beachten, dass dieses Passwort auf der Platte liegt und von jedem der Zugang zum Rechner hat ausgelesen bzw. genutzt werden kann. Durch Cookies lässt sich das Datum des letzten Besuches feststellen. So können dem Anwender nur Dinge angeboten werden, die sich seit dem verändert haben. Durch die Nutzung von Cookies kann man das Surfen teilweise automatisieren lassen und dadurch Zeit sparen. Auch die installierte Software kann hier ein Code ablegen und so erkennt ein Cookie zum Beispiel, welche Version man benutzt und kann so vorschlagen, die neueste Version zu laden.

Sollte man nun Cookies benutzen oder nicht? Auf den generellen Einsatz von Cookies kann wohl kaum verzichtet werden. Andererseits ist es genauso falsch, Cookies immer zuzulassen. Man sollte dabei also wirklich von Fall zu Fall individuell entscheiden.

6 Kryptographie

6.1 Was ist Kryptographie?

Kryptologie ist ein Teilgebiet der Mathematik. Der Begriff ist aus dem griechischen "krypto" abgeleitet und bedeutet soviel wie "verstecken" oder "verbergen". Die Kryptologie beschäftigt sich einerseits damit, Verfahren und Methoden zu entwickeln, die dazu dienen, Daten und damit Informationen vor den Augen Unberufener zu verbergen. Andererseits geht es aber auch darum, Mittel und Wege zu finden, auf Daten, die auf irgendeine Art und Weise verborgen wurden, doch zuzugreifen.

Kryptographie ist der Zweig der Kryptologie, der damit befasst ist, diese Verfahren und entsprechende Techniken zu entwickeln. Dabei geht es jedoch nicht ausschließlich nur darum, Daten vor den Augen Anderer zu verbergen, sondern beispielsweise auch um den Schutz dieser Daten vor Fälschung oder aber auch darum, die Echtheit von Informationen beweisen zu können, ohne diese selbst zu veröffentlichen.

Die Kryptoanalyse versucht, unberufen auf die verborgenen Daten zuzugreifen. Aktive Kryptoanalyse, die gegen staatliche Institutionen oder aber gegen Privatpersonen gerichtet ist, ist in Deutschland verboten.

Allerdings ist die Kryptoanalyse dennoch ein wichtiger Zweig der Kryptologie, da es für einen wirksamen Datenschutz und die dauerhafte Datensicherheit von großer Bedeutung ist, die eventuellen Schwächen verwendeter kryptographischer Verfahren zu kennen. Die Kenntnis dieser Schwächen gewährleistet einen bewussteren und verantwortlicheren Umgang mit wichtigen Daten. Deshalb werden kryptographische Verfahren auf ihre Brauchbarkeit und Sicherheit mittels Kryptoanalyse gegen unbefugte Entschlüsselungsversuche getestet.

6.2 Prinzipielles Verfahren der Kryptographie

Grundprinzip ist die Verschlüsselung und dann wieder Entschlüsselung.

Unter Verschlüsselung, auch Chiffrierung genannt, versteht man die Umwandlung von Daten in eine unlesbare Form. Durch die Verschlüsselung soll verhindert werden, daß jemand die Informationen, die in diesen Daten stecken, erlangen kann, auch wenn ihm die verschlüsselten Daten vorliegen.

Nur befugte Personen sollen eine Zugriff haben. Zu diesem Zweck muss die Verschlüsselung wieder umgekehrt werden. Diesen Prozess bezeichnet man als Entschlüsselung oder Dechiffrierung.

6.3 Warum Kryptographie im Internet?

Das Internet dient der Kommunikation und dem Datenaustausch. Nun besteht zwischen zwei Rechnern, die miteinander kommunizieren, meist keine direkte Verbindung über eine feste Leitung. Statt dessen ist das Internet ein Netzwerk von verschiedensten Rechnern, über die die zu übertragenden Daten geleitet werden, bis sie auf dem Rechner des Empfängers ankommen. Nachteil dadurch ist, daß Daten an den Zwischenstationen abgefangen und gelesen, verändert oder gar unterschlagen werden können. Dies ist jedoch ein großes Problem, wenn man vorhat, vertrauliche Informationen über das Internet zu versenden, z.B. beim Internet-Banking, Online-Shops aber auch bei privater Kommunikation per E-Mail. Deshalb ist es unerlässlich, Kommunikation und Datenübertragung im Internet zu schützen. Um das zu erreichen, setzt man heute immer öfter kryptographische Verfahren in der Internetkommunikation ein.

6.4 Rechtliche Situation

Die Nutzung von Verfahren zur Verschlüsselung von Daten im Internet ist heftig umstritten. Dass sie in Anwendungen bei Online-Shops oder Internet-Banking notwendig und wichtig ist, dürfte jedoch klar sein.

Ein Großteil der über das Internet ausgetauschten Daten und der abgewickelten Kommunikation ist im privater Bereich. Und genau dieser Bereich ist in Bezug auf die Anwendung kryptographischer Verfahren zur Datenverschlüsselung heiß umstritten. Von staatlicher Seite gibt es Bestrebungen, die Verwendung von Kryptographie in der privaten Kommunikation einzuschränken. Und wenn sie nicht verboten werden kann, so soll ihre Anwendung doch wenigstens überwachbar sein.

In Deutschland ist die Situation im Augenblick die, dass es keine gesetzliche Regelung gibt, die den Einsatz kryptographischer Verfahren betrifft. Das bedeutet, dass die Verwendung von Kryptographie nicht verboten ist. Es steht derzeit jedem frei, Daten und Informationen mit einem Verfahren bzw. Programm seiner Wahl, beispielsweise PGP, zu verschlüsseln. Das sieht in anderen Ländern rechtlich ganz anders aus. In den USA unterliegt kryptographische Software sehr strengen Exportbeschränkungen. In Russland sind sowohl die Herstellung als auch die Nutzung jeder Art von Verschlüsselungsvorrichtung ohne den Besitz einer entsprechenden Lizenz verboten.

7 PGP

7.1 Was ist PGP?

PGP ("**P**retty **G**ood **P**rivacy") von Philip Zimmermann ist wohl das bekannteste Freeware Programm zur Verschlüsselung von Dateien.
Mit PGP hat man die Möglichkeit elektronische Post vertraulich zu versenden. Dies wird durch Verschlüsselung der E-Mail erreicht, so dass sie von keiner anderen als der berechtigten Person gelesen werden kann.
PGP biete verschiedene Schlüsselgrößen an: 512bit, 768bit, 1024bit. Im verschlüsselten Zustand sieht die Nachricht aus wie ein bedeutungsloses Durcheinander zufälliger Buchstaben.

7.2 Ein Beispiel

(Datei unverschlüsselt)	**(Datei im verschlüsselten Zustand, Schlüsselgröße: 512 bit)**
Hallo Heiko, ich habe im Lotto gewonnen!	-----BEGIN PGP MESSAGE----- Version: 2.6.3ia hEwD8PEsFxYPIBEBAf9DRCQ5u3JA4Tae1VRmRlNHVQTqiR /HFOc4aFsIB77L4x4B +NMw+4fUY8QEbJhBTjDDgL9COtaEo1q430DSdd6WpgAAAE jFsp9Kd/PZumvskzMQfD61tCS9NMNcY99DexXkTFdRSLDZr BQA+miy1MNe+cpshjLJyYmYjrfxPGcdCz2Y pbEUTUoQNhLxM6k= =cCqq -----END PGP MESSAGE-----

PGP hat seine Fähigkeit bewiesen, sogar den ausgeklügeltesten Analyseversuchen zu widerstehen. Bei einem Versuch einen 48 bit langen Verschlüsselungscode zu knacken, waren 5000 Rechner im Internet verbunden und brauchten dazu 13 Tage. D.h. also, dass ein PGP- Code zu knacken ist, jedoch nur mit enormen Aufwand.
PGP kann auch verwendet werden, um eine digitale Signatur anzubringen, ohne die Nachricht zu verschlüsseln.

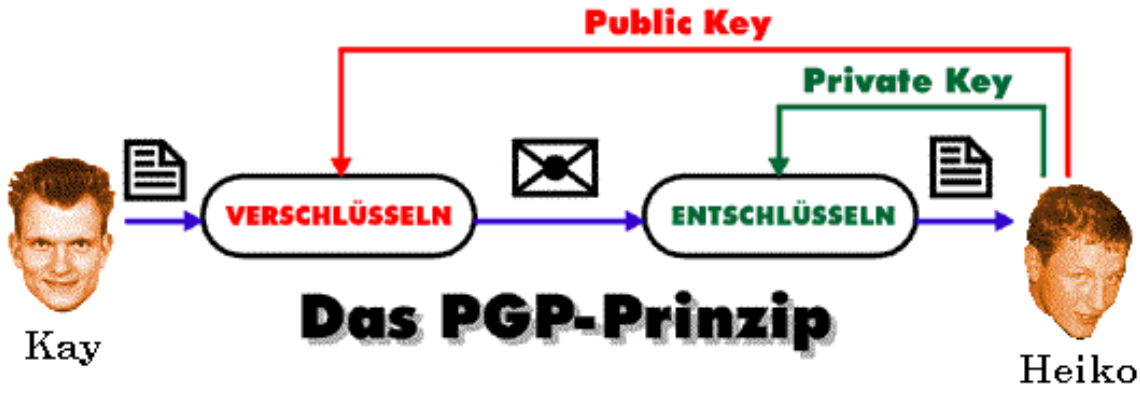
Diese Funktion wird normalerweise in öffentlichen Newsbeiträgen verwendet. Wenn die digitale Signatur erst einmal erzeugt ist, kann niemand mehr die Nachricht oder die Signatur verändern, ohne dass PGP die Manipulation entdeckt.

7.3 Wie funktioniert PGP?

Die Verschlüsselung und Entschlüsselung von PGP setzt sich aus zwei Keys zusammen, dem Public- Key und dem Private Key.
Bei der herkömmlichen Kryptographie wird entweder der selbe Schlüssel für Ver- und Entschlüsselung benutzt, oder es ist auf einfachem Wege möglich, den einen in den anderen Schlüssel zu konvertieren.
Bei der Verschlüsselung mit PGP dagegen mittels Public Key unterscheiden sich die "Chiffrier-" und "Dechiffrier-Schlüssel", und es ist niemandem möglich, den einen in den anderen umzuwandeln. Darum kann der Chiffrier-Schlüssel öffentlich zugänglich gemacht werden und irgendwo in eine Datenbank geschrieben werden. Jeder, der eine Nachricht an jemanden senden möchte, würde seinen Chiffrierschlüssel aus dieser Datenbank oder anderswoher beziehen und seine Nachricht an ihn verschlüsseln. Die Nachricht kann nicht mit dem Chiffrierschlüssel entziffert werden! Daher kann niemand, außer dem dazu berechtigten Empfänger die Nachricht entschlüsseln. Noch nicht einmal die Person, die den Text verschlüsselt hat, kann den Prozess umkehren. Wenn man eine Nachricht empfängt, benutzt man seinen privaten Dechiffrier-Schlüssel um die Nachricht zu entziffern. Dieser geheime Schlüssel verlässt niemals den Computer. Selbst der geheimer Schlüssel ist selbst verschlüsselt um ihn vor jedem, der am Computer herumschnüffelt, zu schützen.

7.4 Wie ist der Ablauf?

Heiko erzeugt sich ein Schlüsselpaar, das zur Verschlüsselung und Entschlüsselung von Nachrichten dient. Seine Public Key legt er in ein für alle zugängliches Depot oder verschick ihn an mich. Wird nun eine private Nachricht an Heiko geschickt, verschlüsselt Kay die Nachricht mit Heikos Schlüssel. Wenn Heiko die Nachricht erhält, entschlüsselt er sie mit seinem Private Key. Kein anderer Empfänger kann diese Nachricht entschlüsseln, weil nur Heiko seinen persönlichen Code kennt.



8 Bezahlen im Internet

8.1 Allgemeines

Eine Sensationsmeldung im Januar schreckte viele Online Kunden auf. Es kam zum bislang größten Diebstahl von Kreditkartennummern über das Internet. Ein russischer Hacker hatte versucht, von einem amerikanischen Online- Musikversandhandel 100 000 Dollar zu erpressen, und gab an, im Besitz von 300 000 gültigen Kreditkartennummern von Kunden des Versandes zu sein.

Als das Unternehmen nicht zur Zahlung bereit war, begann der Hacker die Nummern zu veräußern. Nachdem 25 000 Nummern veröffentlicht wurden, gelang es dem FBI die Seite zu schließen. Wie der Hacker an die Daten gekommen war, ist noch unklar; vermutet wird ein Programmfehler in der E-Commerce- oder Datenbanksoftware.

Dieses Beispiel zeigt Gefahren des Online-Handels. Kreditkartennummern sind begehrte Daten, die professionelle Trickdiebe z.B. aus Papierkörben von Tankstellen oder Hinterzimmern von Restaurants sammeln. Bei nötigem Wissen und Geduld sind Nummern auch errechenbar. Ein häufiger Trick um im Internet an Kreditkartennummern zu kommen, ist die Nummernabfrage als Altersnachweis, um Zugang zu entsprechenden Seiten zu erhalten..

Prinzipiell sind Geschäfte im Netz auch nicht betrügerischer als andere, doch durch unpersönliche Geschäftsbeziehungen sinkt die Hemmschwelle auf ein Minimum. Der Missbrauch von Kreditkarten ist inzwischen zum häufigsten Vergehen im Internet geworden.

Dem Kunden drohen grundsätzlich drei Gefahren:

- Daten können während der Kommunikation zwischen Händler und Kunden von Dritten ausspioniert werden,
- Diebe eignen sich Nummern durch Einbruch in Server oder PC an

- Käufer wird vom Händler betrogen

Deshalb, sollte man sich vor einem Online Geschäft erst einmal informieren, wer hinter der angegebenen Adresse steckt. Ist es vielleicht ein bekanntes Unternehmen? Wie sieht das Warenangebot aus und sind die Geschäftsbedingungen klar und verständlich.
Auf jeden Fall sollte man nie unverschlüsselt Daten übermitteln!
Den Kaufvertrag immer gründlich lesen und auf Details bei Rückgaberecht und Versandkosten achten! Sollte einmal etwas mit der Kreditkartenrechnung nicht in Ordnung sein, ist der Kunde recht gut geschützt, Stornierung bei der Bank sind möglich, es kann aber Wochen dauern bis das Geld wieder auf dem eigenem Konto ist.
Beim Zahlungsverkehr zwischen dem Kunden und dem Händler unterscheidet man in der Regel 2 Methoden. Kommunizieren Käufer und Verkäufer direkt miteinander, bezeichnet man diesen Vorgang als Offline E-Cash. Ist dagegen ein Vermittler (z.B. Bank) zwischen beiden Parteien tätigt, wird das ganze als Online E-Cash bezeichnet. Eines von vielen modernen Verfahren, soll im folgenden näher erläutert werden.

8.2 SET (Secure Electronic Transaction)

Set ist ein Standard -verfahren der Kreditkartenzahlung.
Das System wurde von Eurocard/ Mastercard und Visa gemeinsam mit IBM, Microsoft und Netscape entwickelt.
Bevor der interessierte Kunde aber das System nutzen kann, ist ein gewisser Verwaltungsaufwand notwendig. Wie bei einer Kreditkarte muss auch für das Set -System ein Vertrag geschlossen werden. Danach bekommt der Kunde dann Software von seiner Bank, die er dann auf seinem PC installieren sollte. Durch die Software stehen dem Kunden dann sogenannte Wallet zur Verfügung, eine Art elektronische Brieftasche, in der auch mehrere Kreditkarten verwaltet werden können.
Zusätzlich bekommt der Kunde eine persönliche Identifikationsnummer die anstatt der Kreditkartennummer übertragen wird. Auch der Händler muss für SET zertifiziert sein, und benötigt entsprechende Software.
Alle Daten die übermittelt werden, sind RSA -verschlüsselt, die nach dem Schloss-Schlüssel -Prinzip dafür sorgt, dass die Informationen während des Transfers nicht abgelesen oder verfälscht werden können.

Der Händler rechnet mit Kreditunternehmen ab und dieses wiederum mit dem Kunden. Dadurch erfährt der Händler keine Kartennummern mehr! Auch gibt es keine zentrale Instanz mehr, die alle öffentlichen Schlüssel verwaltet, sondern eine Hierarchie von CA's (Certifikation Authorities). Dadurch sinkt das Risiko, von der eigenen Bank ausspioniert zu werden.

8.3 Ein Beispiel

Ein Kunde bestellt beim Händler bestimmte Waren. Daraufhin übermittelt der Händler dem Kunden die Transaktionsnummer, Händler -Zertifikat und Zertifikat des Gateways des Kreditkartennetzes der Händlerbank. Nun muss der interessierte Kunde sein persönliches Kundenzertifikat und die digital unterschriebene Bestell -und Zahlungsinformation in einem digitalen Kuvert, welches nur von der Händlerbank zu öffnen ist, zurücksenden.
Der Händler überprüft Kundenzertifikat und digitale Signatur, wenn alles in Ordnung ist, wird die bestellte Ware abgeschickt. Die Händlerbank führt einen Kundenauthorisierungsprozeß mit der Kundenbank durch, worauf der Händler eine beglaubigte Rechnung an den Kunden verschickt.
Ein Nachteil ist, dass das System momentan noch sehr wenig im Online- Handel verbreitet ist.
Ein großer Vorteil ist, es werden nicht nur die verschlüsselten Daten sicher übertragen, sondern auch gleichzeitig die Absender überprüft.

9 Zusammenfassung

Wie man sieht, sollte man sich der Gefahren im Internet bewusst sein. Denn wie wir gesehen haben, lauern sie überall. Einerseits kann man beim Surfen viel von sich Preis geben, andererseits ist der Rechner vor Angriffen aus dem Netz meistens nicht geschützt. Deshalb ist es ratsam einige Sicherheitsvorkehrungen zu treffen, besonders wenn man von einem Firmenrechner aus sich im Internet beschäftigt. Am Privat – PC sollte man ständig darauf achten, was man sich aus dem Internet herunterlädt, dabei helfen Antivirenprogramme. Das das viele Internetuser nicht machen ist verständlich, da sie nach dem Motto handeln: „Für meinen Computer interessiert sich sowieso keiner“. Das kann zwar durchaus der Fall sein, aber bei Viren, die per Massensendungen verschickt werden, wird eine Vielzahl von Computern gleichzeitig erreicht, wie wir an dem Beispiel aus der Einleitung gesehen haben. Wenn man sich also entsprechend schützt steht einem Internetvergnügen nichts mehr im Wege.

Quellenverzeichnis

- www.bsi.de Homepage des Bundesamtes für Sicherheit in der Informationstechnik
- www.bingo-ev.de/~ub304/cookies.htm Alles über Cookies
- www.raven.to/cookie Cookies - Digitale Krümel im Netz
- www.cityweb.de/free/3.spam100499.inhalt-000.html Alles über Spam
- www.cert.dfn.de/team/ue/fw/workshop/workshop.html
- www.iks-jena.de/mitarb/lutz/anon/pgp.html Nichttechnische Einführung zu PGP
- www.iks-jena.de/mitarb/lutz/security/pgpfaq.html
- www.muenster.de/~marvel/default.html Offiziele PGP-Leitseite der Universität Muenster
- pgp.gildemax.de Das Verschlüsselungsprogramm PGP was ist PGP, - wie funktioniert PGP, - wo erhält man PGP
- www.fitug.de/ulf/krypto Alles über Kryptographie
- www.iks-jena.de/mitarb/lutz/security/cryptfaq Kryptographie FAQ 3.0
- www.educat.hu-berlin.de/publikation/student/kryotologie

Besuchszeit dieser Internetseiten: 5/2000

Jürgen Borngießer, Unheimliche Besucher, Internet Magazin 6/2000, 48;
Christian Köhntopp, Alles Dicht, IX 5/2000, 50;
Ralf Hüskes, Versiegeln, IX 5/2000, 56;
Jürgen Seeger, Gezielte Abwehr, IX 5/2000, 62;
U.Eike, WWWölfe im Schafspelz, CHIP 6/2000, 194;
M.Flohr, Gefährliche Einkauftouren, CHIP 3/2000, 236;
Andreas Maslo, Sichere Festung, PC Magazin 5/2000, 170;
Burckhart Müller, Tag der offenen Tür, PC Magazin 5/2000, 166;
Burckhart Müller, Surfen mit Rettungsring, PC Magazin 2/2000, 196;