Gesellschaftliche Aspekte der Informatik

Thema: Schnüffelprogramme und Abhörsysteme

Stefan Müller, Marco Sorich, York Krausse und Stephan May
FH-Brandenburg SS2001

Einleitung

Immer mehr Menschen finden Zugang zum Internet, nutzen es regelmäßig, z.B. um sich einfach nur zu Informieren, aber auch um Online-Banking zu betreiben oder mal schnell ein Buch zu bestellen.
Leider ist den meisten nicht bewußt, das auch andere Internetsurfer so Zugang auf ihren Rechner erhalten und auch nicht welche Informationen sie beim Surfen hinterlassen bzw. senden.
Um sich dagegen schützen zu können, muß man sich zunächst darüber informieren, was mit den Daten im Netz passiert und auch welche Möglichkeiten ein „Spion“ hat, um an diese zu gelangen.

Wir haben uns deshalb mit den eigentlichen Angriffsmöglichkeiten beschäftigt und haben bereits bei der Vorstellung unseres Themas gezeigt, wie einfach man den Datenverkehr in einem lokalem Netzwerk abhören kann und so leicht z.B. zu Paßwörtern kommt.

1. Spionage am Arbeitsplatz
2. Anonymität im Internet

Für den Surfer wird es allerdings schwierig sich zu schützen, wenn hinter dem Angreifer mächtige Organisationen stecken, die ein großes Abhörsystem betreiben, das nicht nur das Internet belauscht, sondern auch den gesamten Telefon- und Faxverkehr.

Zwei aktuelle Themen dazu sind Carnivore, ein Programm, das den gesamten E-Mailverkehr durchsucht, und
ECHELON, ein weltweites Abhörsystem.
Beides hat in jüngster für große Aufregung in der Welt gesorgt, vor allem in Europa.

3. Carnivore – Ein Raubtier im Internet ?
4. Echelon

Spionage am Arbeitsplatz

zum Inhalt

Einleitung

Was sind Schnüfflerprogramme ?

Wie arbeiten sniffer?

Ein Beispiel

Wie kann man sich schützen?

Einleitung

Das Mitlesen von Datenübertragungen wird dem Angreifer sehr leicht gemacht.
Je nach Wunsch kann er sich Passwörter und Zugangskennung von Arbeitskollegen erschleichen, fremde Emails mitlesen, anderer Leute Surfgewohnheiten studieren, ja jeglichen Netzwerkverkehr eines oder mehrerer User mitloggen. Und das alles unerkannt.

Viele User verlassen sich auf den Schutz durch ihre Passwörter. Sie wiegen sich in Sicherheit. Nun ist auch das Gewirr der Begriffe für die meisten Endanwender undurchschaubar. Wir kennen dutzende Protokolle und Dienste ,
SMTP, POP3, IMAP, HTTP, HTTPS, FTP, NNTP. Was bedeuten sie und wie sicher sind sie ? Welche davon sind anderen vorzuziehen?
Es macht Spaß sich im Intranet und Internet zu bewegen und all seine Möglichkeiten auszukosten. Die wenigsten Anwender und leider auch Administratoren sind sich jedoch über die kriminelle Energie einzelner Mitarbeiter und deren Möglichkeiten bewußt.

In PC-Zeitschriften und im Internet gibt es zahllose Artikel und Tools. Die Vorgehensweise und Anwendung ist genauestens beschrieben. Jeder kann somit zum Spion werden. Jeder der anderen Mitarbeiter könnte gerade jetzt schnüffeln.

Das allgemeine Ziel ist es, Logins und Passwörter zu ermitteln. Danach ist es ein Leichtes, sich als anderer Benutzer auszugeben, fremde Transaktionen zu starten, oder fremde Daten einzusehen.
Am Anfang stehen Schnüfflerprogramme.

Was sind Schnüfflerprogramme

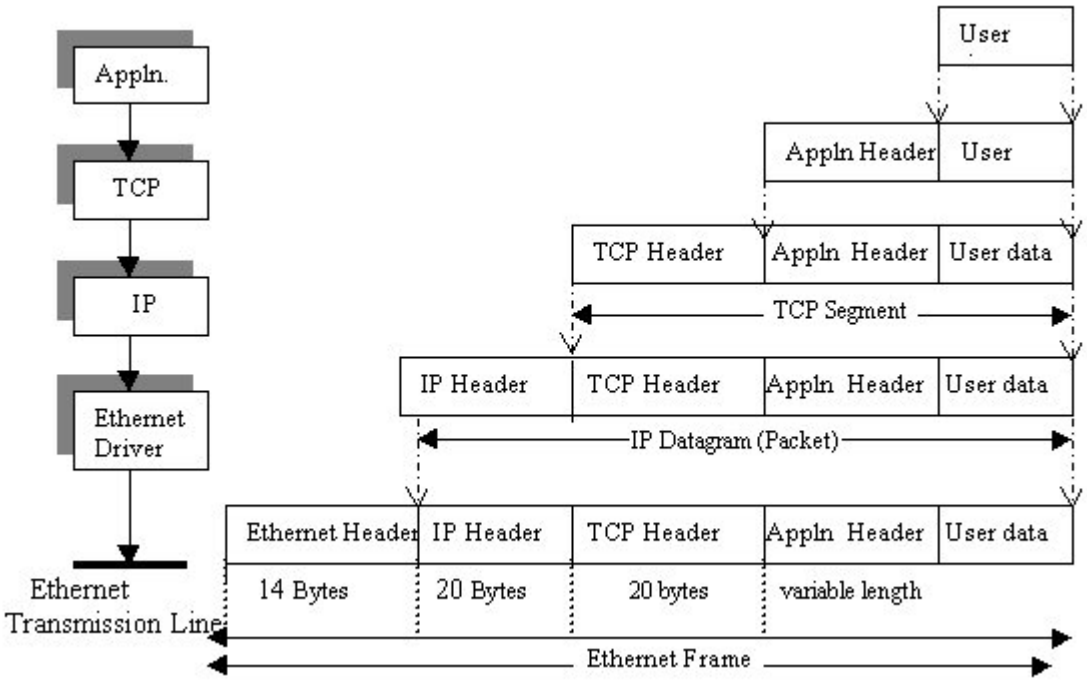
Schnüfflerprogramme im Englischen als sniffer bezeichnet, sind kleine Programme mit großer Wirkung. Sie können den kompletten Netzverkehr in Dateien speichern und analysieren. Mußte man sich früher noch mit dem Aufbau von Netzwerken und Protokollen auskennen, so ermöglichen heute gut gestaltete GUIs den intuitiven Einsatz.

Sniffer werden immer mit negativen Aspekten in Verbindung gebracht. Dabei wird deren eigentliche Anwendung unterschlagen. In ihrer Funktion als Protokollanalyser sind sie ein wichtiger Bestandteil beim Aufbau, Test und Fehlererkennung von Netzwerken unumgänglich auch bei der Entwicklung von Netzwerkapplikationen, eigenen Protokollen und bei der Prüfung von sicherheitstechnischen Aspekten. Aus der Entwicklung und Weiterentwicklung von rechnergestützter Kommunikation sind sie nicht wegzudenken.

Wie arbeiten sniffer?

Aus den Grundlagen des Netzwerkmanagementes kennen wir das ISO-OSI-Modell.
Die physikalische Schicht (Layer 1) steht für die Bitfolgen, die in den Kabeln und in den Netzwerkkarten laufen. Die aufbauenden Schichten sind zur Adressierung und Kapselung der Daten. Sie dienen zur Zielbeschreibung sowie der Sicherstellung des korrekten

Inhaltes.



Dieser geschachtelte Aufbau hilft bei der Übertragung.
Diejenigen Pakete, die nicht an einen Rechner adressiert sind, werden von ihm einfach ignoriert und damit nicht weiterverarbeitet. Das gewährleistet zum einen die geringere Auslastung des PCs und zum anderen eine gewisses Stück Sicherheit bei der Kommunikation.
An dieser Stelle setzt jetzt der sniffer ein. Die Netzwerkkarte schaltet in einen anderen physikalischen Modus - den promiscuous-mode. Das hat zur Folge, daß alle Pakete, die sich auf der Leitung bewegen, bearbeitet werden. Mit anderen Worten, mich erreichen damit Informationen, die nicht für mich gedacht sind. Ich sniffe fremden Netzverkehr.
Die unterschiedlichen Dienste nutzen jeweils spezielle Protokolle. Mit Kenntnis über die Eigenarten ist es sehr leicht spezifische Informationen zu filtern und Spionageangriffe zu starten.

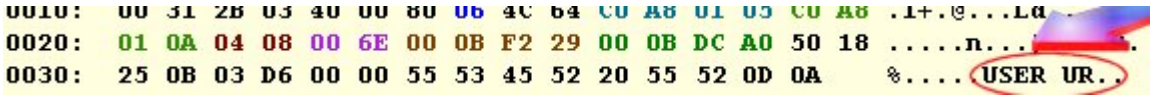
Ein Beispiel

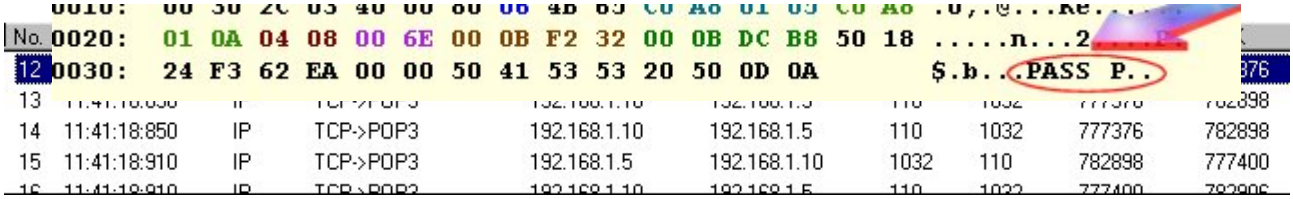
Zum Versuch baue ich ein kleines TCP/IP- Netzwerk auf. Ich starte einen POP3 - und einen HTTP- Server. Dann frage ich mit meinem Browser diese Server ab und zeige den Datenaustausch. Dabei sniffe ich mit den Tools CaptureNet und PeepNet.

Was sehe ich ?

Die komplette Kommunikation, Anfragen und Antworten, wurde mitgeschnitten.
Ich greife mir jetzt die 2 entscheidenden Pakete heraus.

Wie schon in der Abbildung der Layer gezeigt, werden noch andere Daten übertragen. Für die Demonstration interessiert uns der letzte Teil des Paketes. Bei der POP3-Kontoabfrage wird der Inhaber mittels "USER" und "PASS" identifiziert.





Die Daten werden im Klartext übertragen ...
Und ab jetzt wäre der schnüfflende Kollege im Nachbarraum so schlau wie ich - was zumindest Benutzernamen und Passwort betrifft. User "UR" hat das das Passwort "P".
Und es kann noch weiter gehen ...
Das Verfolgen meiner Internetaufrufe ist ebenso leicht. Diesmal beobachten wir das HTTP.



Im folgenden surfen wir mit dem Analysetool sogar die gleichen Seiten an.



Wie kann man sich schützen?

Sniffer gibt es für alle Plattformen, deshalb ist das noch kein Beitrag zur Sicherheit. Der Administrator hat die Möglichkeit in seinem Netzwerk nach Karten im promiscuous-mode zu suchen. Die sogenannten Antisniffer stellen den Angreifer.

Als Anwender ist folgendes zu beachten. Sobald die Möglichkeit besteht mit sicheren Übertragungen zu arbeiten, sollten diese genutzt werden. Viele Anbieter stellen bei ihren Seiten den HTTPS Zugang zur Verfügung. Ein schönes Vorbild ist hier der Chaos Computerclub: https://www.ccc.de.
Ebenso wichtig ist der Gebrauch von POP3S sowie SMTPS um den Emailtransfer zu sichern.
Viele nützliche tools sind unter http://www.openssh.org auch kostenlos zu beziehen.
Gleichzeitig ist der Einsatz von Verschlüsselungsprogrammen wie zum Beispiel PGP zu empfehlen.

Quellen

Datenschutz - CD
http://www.utechmedia.net

diverse Internetseiten über Netzwerke, Dienste und Protokolle

Tools

CaptureNet - network sniffer for Windows 95/98/NT.
PeepNet - comes along with CaptureNet

Anonymität im Internet

No matter how paranoid you are, you are not paranoid enougth.
Steve Bass

0. Einführung 1
1. Angriffsmöglichkeiten 1
1.1. Cookies 1
1.2. Web-Bugs 2
1.3. Spyware 3
1.4. Portscan 3
1.5. DoS-Attacken 4
1.6. Java-Applets 4
1.7. Active-X 4
2. Präventions-Möglichkeiten 5
2.1. Cookie-Management 5
2.2. Inhalts-Filter 5
2.3. Firewalls 6
3. Angriffs-Szenarien 6
3.0. Vorbemerkung 6
3.1. Die IP des Opfers ermitteln 6
3.1.1. Mit Hilfe des AOL-Instant-Messanger 6
3.1.2. Mit Hilfe des ICQ 6
3.1.3. Mit Hilfe des IRC 6
3.1.4. sonstige Möglichkeiten 7
3.2. Angreifen 7
3.3. Nachwort 7

0. Einführung

Wie allgemein bekannt, ist es mit der Anonymität im Internet wirklich schlecht bestellt. Jeder der im Internet surft gibt unweigerlich eine Menge an Informationen von sich preis. Aus diesem Grunde halte ich es für außerordentlich wichtig, dass sich jeder Surfer nicht nur darüber im Klaren ist, sondern sogar weiß was über ihn in Erfahrung gebracht werden kann und wie das geht.

Dieser Text beschreibt einige Punkte wie Firmen (z.B. einige Werbebanner-Firmen) persönliche Daten, den Festplatteninhalt des heimischen Rechners oder das Surf-Verhalten des Users mitprotokolieren. Er erhebt keineswegs den Anspruch auf Vollständigkeit, es sollen jedoch einige beispielhafte Formen des Mitprotokolierens kurz vorgestellt werden.

1. Angriffsmöglichkeiten

1.1. Cookies

Cookies sind bekanntlich nichts weiteres als Informationen die ein Betreiber einer Webseite auf dem Rechner des Surfer ablegen kann. Diese Informationen werden dann vom Browser gespeichert und beim nächsten Aufruf eben dieser Webseite auf Anfrage wieder zu der Seite zurückgeschickt. Ein Cookie könnte zum Beispiel folgendermaßen aussehen:

```
WEBTRENDS_ID-2257931092.29358898
202.155.27.16
-2257931092.29358898
facelink.snap.com
0 2865430528 30123157 1534254528 29358607 *
```

In diesem Cookie erkennt man zum einen die IP, die man selbst hatte, als man online war. Dadurch lässt sich z.B. schon mal ermitteln, über welchen Provider man online war und auch meistens für gewöhnlich geht. Man erkennt außerdem die Internetadresse der Website, die dieses Cookie angelegt hat, sowie einige kryptisch aussehende Zahlen, die irgendwelche Informationen über den Surfer enthalten.

Der Hintergrund ist zum Beispiel dass man – einmal eingeloggt – sich nicht ständig wieder erneut mit Username und Passwort einloggen muss, oder dass ein Besucher einer Shopping-Seite von dieser wiedererkannt wird und ihm für ihn interessante Angebote unterbreitet. Dabei hat der Surfer meist vorher schon ein langes Profil ausgefüllt, in dem nicht nur Name, Adresse, Telefonnummer, Mail-Adresse usw. gefragt sind, sondern auch Vorlieben, Interessen, Hobbys, monatliches Bruttoeinkommen etc. Das sind z.T. schon wirklich persönliche Daten, die nicht unbedingt in die Hände, möglicherweise unseriöse, Dritte geraten sollten.

Das erste Sicherheitsproblem kann sich schon alleine daraus ergeben, das andere Personen Zugriff auf den eigenen Rechner haben und sich demnach gegenüber einer Website, die ein Cookie abgelegt hat, als der eigentliche User identifizieren. Auf dieses Problem wird im Text allerdings nicht weiter eingegangen, weil der Schutz vor unbefugten lokalem Zugang auf den eigenen Rechner nicht Inhalt dieser Ausarbeitung sein soll.

Nun schickt ein Browser unter normalen Umständen allerdings meist nur die Cookie-Inhalte an die Seite zurück, die auch dieses Cookie abgelegt hat. Es kann also keine Webseite einfach mal alle Cookies abfragen (unter normalen Umständen). Wenn man sich allerdings mal seine Cookiesammlung durchschaut (bei den Cookies vom Internet Explorer ist das möglich, Netscape speichert alle in einem File), wird man viele Cookies finden, die von Webseiten stammen, die man noch nie im Leben besucht hat (die Internetadresse von dem das Cookie stammt steht mit in diesem drin). Wo kommen also diese Cookies her? Die Erklärung ist ganz einfach: enthält eine Webseite Grafiken, die von einem anderen Server (und somit einer anderen Webseite) stammen, ist dieser andere Server auch berechtigt Cookies abzulegen. So etwas bezeichnet man als einen *Web-Bug*. Hin und wieder sind auch gar nicht mal Werbebanner die Übeltäter, als eher unsichtbare 1x1-Pixel große transparente Grafiken, die der nichtsahnende Surfer gar nicht mal zu Gesicht bekommt. Zusätzlich sind Cookies in der Lage die Eingaben, die man in einem Webformular macht, mitzutracken. Somit kann also ein Cookie, z.b. von einem Werbebanner, sämtliche Eingaben in eines der oben erwähnten Profile mitverfolgen und diese dann der Werbefirma zur Verfügung stellen. Nebenbei können Cookies auch noch den weiteren Weg des Surfer durch das Internet verfolgen, womit sich schnell ein gutes Surfprofil über bevorzugte Seiten bzw. Seiteninhalte, Aufenthaltsdauer usw. erstellen lässt, sofern der Surfer schon mal bei einer Seite vorbeischaut, die eine Grafik des gleichen Servers enthält. Wenn Firmen diese Daten dann auch noch mit gesammelten persönlichen Informationen über Name, Telefonnummer, Einkommen etc., und regelmäßig abgefragten E-Mail-Konten verbindet, sind diese Informationen anderen Firmen, wie beispielsweise Spam-Mail-Firmen, schon mal etliche tausend US-Dollar wert.

1.2. Web-Bugs

Web-Bugs sind aber nicht nur für Cookies zuständig. Sie können noch wesentlich mehr. Grundsätzlich ist die Verwendung von Web-Bugs gar nicht auf HTML-Seiten beschränkt, sondern sie können in jeder Art Dokument vorkommen – seien es E-Mail, Word-, Excel, Po-

werpoint-Dateien, pdf-Files etc. Dabei hat das noch nicht einmal mit angeblich schlechten Sicherheitsvorkehrungen von Office-Paketen oder so was zu tun. Alle Dateien die Verweise auf Grafiken enthalten können, machen dies meist in Form einer URL, also einer ganz normalen Internetadresse. So eine Internetadresse kann allerdings auch auf die eigene Festplatte zeigen, wenn man z.B. schreibt: „file://c:/“. In diesem Falle zeigt die URL auf das Hauptverzeichnis der Platte C: des eigenen Users. Somit ist es völlig egal, wo die Grafik liegt – im Internet, oder auf der eigenen Platte, und wenn man sowieso gerade online ist merkt man gar nichts davon, dass die Grafik soeben aus dem Internet geladen wurde und damit gleichzeitig einige Informationen an den Server, auf dem die Original-Grafik liegt, geschickt wurde (wie möglicherweise IP, aufrufendes Programm, Dateityp, Betriebssystem, Username, Email-Adresse, offene Ports, etc.). Das ganze klappt auch genauso gut, wenn man sich seine Emails online durchliest, woraufhin der User dann in Zukunft mit Newslettern bombardiert werden kann.

Andererseits kann man mit Hilfe der Web-Bugs auch eine Art von Copyright-Information realisieren. Die kann z.B. in Firmen dazu benutzt werden zu überprüfen, wer welche vertraulichen Dokumente an wen weiterleitet.

1.3. Spyware

Seit noch nicht all zu langer Zeit ist es in die Mode gekommen, dass Programmierer von Shareware- oder Freeware-Tools ihre Programme mit der Möglichkeit versehen, dass diese sich einerseits vom Internet Werbung herunterladen können und andererseits statistische Informationen an die Werbe-Firma übertragen. Auf diese Weise lässt sich schnell mal ein nicht zu aufwendiges Freeware-Projekt finanzieren. Dabei nehmen diese Programme bei bestehender Internet-Verbindung eigenständig Kontakt zu „ihrer“ Website auf und übertrage dabei die entsprechenden Informationen. Obwohl alle Hersteller dieser Spyware möglicherweise hoch und heilig versprechen, dass ihre Programme keine persönlichen Daten übertragen, ist eine eigenständige und unabhängige Überprüfung dieser Behauptung meist doch recht schwierig bzw. teilweise unmöglich (z.B. wenn diese Informationen komprimiert oder verschlüsselt übertragen werden).

Einige Programme sind dabei sogar in der Lage sich selbständig ins Internet einzuwählen und eine Verbindung zum Hersteller aufzubauen. Andere wiederum integrieren sich so in das bestehende System und in den Standard-Browser, dass sie sich nicht mehr deinstallieren lassen.

1.4. Portscan

Oftmals wird der eigene Rechner allerdings auch „direkt“ aus dem Internet angegriffen, also nicht erst, wenn sich ein anderes Programm, ein Cookie oder etwas ähnliches meldet. In so einem Fall ist meist die Vorform einer solchen Attacke ein sogenannter *Portscan*. Mit diesem wird der Rechner auf benutzte und ungeschützte Ports geprüft, ob z.B. ein Instant-Messanger oder eine Festplatten-Freigabe unter Windows, ein Web- oder FTP-Server, oder so etwas verfügbar ist, das womöglich einen Einbruch in das System ermöglicht. Wenn erst mal alle Ports des Opfers bekannt sind, die sich von außen ansprechen lassen, kann man in Ruhe ermitteln, welche sich am besten zum Einbruch eignen. Dazu werden evtl. die Versions-Nummern der Server oder Messanger ermittelt, woraufhin im Internet genügend Informationsmaterial zu finden ist, zu welcher Version bei welchem Programm, welche Sicherheitslücken gefunden wurden. Nicht zu unterschätzen ist auch die Gefahr, von möglichen Trojanern, die man sich unbemerkt aus dem Netz gezogen haben könnte, und die längst tief im System verankert sein könnten und auf sonst immer ungenutzten Ports ins Internet lauschen.

1.5. DoS-Attacken

Diese Attacken (Denial of Service) dienen einzig und allein dazu eine Firewall oder einen Server außer Gefecht zu setzten, um beispielsweise an einer Firewall vorbeizukommen. Dazu sendet der Angreifer innerhalb weniger Sekunden tausende von Anfragen (im einfachsten Fall nur ICMP-Anfragen). Dann kann es sein, dass das entsprechende System nicht mehr in der Lage ist alle rechtzeitig zu überprüfen und es total, oder für kurze Zeit (ein paar Sekunden) ausfällt und damit den Weg ins System freigibt.

1.6. Java-Applets

Java-Programme, die als Applet auf den Rechner geladen werden, sollten eigentlich nur innerhalb einer sogenannten Sandbox ablaufen. Das würde bedeuten, dass die Funktionalität eines solchen Applets gegenüber normalen Java-Applikationen stark eingeschränkt sein sollte und keinerlei Möglichkeiten existieren sollten auf das Dateisystem, angeschlossene Peripherie, vorhandene Netzwerkressourcen oder auf andere sicherheitsrelevante Bereiche zuzugreifen. Sobald ein Applet jedoch nach solchen Rechten verlangt, wird dies meistens nicht automatisch verweigert, sondern der Surfer bekommt Warnmeldung angezeigt (sofern er seinen Browser wenigstens darauf eingestellt hat), welche meist lediglich harmlos umschreibend nach „full permissions“ fragt, aber keineswegs darauf hinweist, dass das durchaus große Gefahren mit sich bringen kann (siehe Abbildung 1 – hier die Meldung des Internet-Explorers).



Abbildung 1

Nachdem der User diese Frage nun positiv (im Sinne des Applets) beantwortet hat, steht dem Zugriff auf sicherheitsrelevante Bereiche nichts mehr im Wege. Man sollte sich als Surfer also immer vor dem Beantworten die Frage stellen, *wer* hier nach vollen Rechten verlangt (ist es die eigene Bank zum Homebanking over Internet oder womöglich ein mysteriöses Werbebanner). Es ist natürlich dafür notwendig, dass der Browser darauf eingestellt ist, nicht automatisch alle Rechte zuzulassen, sondern (wenn überhaupt) erst auf Nachfrage.

1.7. Active-X

Als eine Erweiterung aus dem Hause Microsoft bietet sich Active-X als Einbruchs-Möglichkeit geradezu an, da dieses nicht nur der Verschönerung von Internet-Seiten dient (aber durchaus auch), sondern ebenso zur automatisierten Steuerung von Windows. Aus diesem Grunde hat man als Active-X-Programmierer Zugriff fast auf die komplette Win-API.

Bei entsprechender Konfiguration des Browsers wird man zwar vor dem Ausführen von solchem Code nach derer Genehmigung gefragt, aber etwas vergleichbares, wie bei Java-Applets die Sandbox, gibt es hier nicht. Mit anderen Worten: ganz oder gar nicht. Das ist sehr bedauerlich, weil ein Active-X-Programm unsichtbar Tastaturanschläge an jedes beliebige Programm senden kann, nachdem es dieses gestartet hat – so, als würde dieses per Tastatur von dem vor dem Rechner sitzenden User bedient werden (dazu ein Bericht des CCC unter http://www.heise.de/ix/artikel/1997/03/090/).

Eine auf den ersten Blick sehr nützlich erscheinende Sicherheitsvorkehrung hat Microsoft allerdings eingebaut – wohl aber scheinbar mehr um Geld zu verdienen und nichts ahnende Surfer zu irritieren, als tatsächlich Sicherheit zu gewähren. Ein Programmierer kann sich nämlich für 20 US-Dollar eine Acitve-X-ID kaufen, mit der er sein selbstgeschriebenes Programm signieren kann. Eine entsprechende Meldung auf dem Bildschirm des Surfers, ob er ein *signiertes* Active-X-Control ausführen lassen will, suggeriert sehr schnell ein von Microsoft als nicht schädlich freigegebenes und überprüftes Control, was allerdings nicht so ist.

Mindestens genau so schlimm ist die Tatsache, das, für die Ausführung von Active-X-Controls evtl. benötigte DLL's, die sich noch nicht auf dem System befinden, automatisch und im Hintergrund bei ftp.microsoft.com runtergeladen werden.

2. Präventions-Möglichkeiten

2.1. Cookie-Management

Viele Browser – dazu gehören derzeit (November 01) definitiv Opera und Internet Explorer ab Version 6 – ermöglichen ein sogenanntes Cookie-Management. Bei diesem kann man gezielt einstellen wie man mit Cookies umgehen möchte. Es wird unterschieden zwischen Cookies von dem eigenen Server, von der eigenen Domain und von Drittanbietern (z.b. Werbebannern). Wobei der Unterschied der zwei erst genannten der ist, das einige große Service-Anbieter durchaus über mehrere Domains auf dem gleichen Server verfügen können (beispielsweise aol.de, www.aol.de und aolmail.aol.de). Des weiteren kann man Domains oder Server angeben von denen definitiv immer alle Cookies akzeptiert oder verweigert werden.

Es ist wirklich ganz sinnvoll sich dieser Möglichkeit anzunehmen und mal drüber ein paar Online-Hilfen oder Internetseiten zu bemühen. Man kann damit dann nämlich beispielsweise alle notwendigen Cookies bei einem Internet-Kauf annehmen wobei allerdings alle die der Werbebanner oder Web-Bugs abgelehnt werden, ohne das man tausend-mal explizit danach gefragt wird.

2.2. Inhalts-Filter

Es gibt auch Programme (z.b. den Webwasher), die eingehende Internetseiten parametrisiert auf ihren Inhalt prüfen und entsprechende Sachen herausfiltern. Dazu können Cookies zählen, sowie Web-Bugs, Active-X- und Java- oder JavaScript-Elemente. Einige unterstützen dabei sogar noch das oben genannte Cookie-Management, oder erweitern das von Java bekannte Sandbox-Prinzip auf alle anderen HTML-Elemente. Meistens funktionieren solche Programme als Proxy, auf welchen der Browser dann erst eingestellt werden muss.

2.3. Firewalls

Firewalls protokollieren den ein- und ausgehenden Datenstrom und überprüfen anhand einer eingestellten Konfiguration ob die ein- und ausgehenden Pakete überhaupt gestattet sind bzw. Informationen enthalten, die nicht ins Internet geschickt werden sollen. Es gibt neben den kommerziellen Firewalls auch einige (für den Privatanwender) als Freeware erhältliche Produkte (z.B. von Sygate die SPF, oder ein Produkt Namens ZoneAlarm, welche über Suchmaschinen im Internet zu finden sind), die durchaus für den Privatgebrauch tauglich sind. Dabei unterscheiden sie sich in der Flexibilität des Konfiguration und damit auch in dem Aufwand und der Komplexität der Bedienung. Einige prüfen lediglich den Datenstrom der einzelnen Ports, andere wiederum unterscheiden, welche Programme welche Ports nutzen dürfen und es gibt auch welche mit integrierten Inhalts-Filtern und Viren-Scannern.

3. Angriffs-Szenarien

3.0. Vorbemerkung

Im folgenden wird beschrieben wie man einen Angriff gegen ein bereits ausgesuchtes Opfer startet.

Ich möchte an dieser Stelle allerdings ausdrücklich darauf hinweisen, dass ich mit dem Beschreiben von möglichen Angriffs-Szenarien nicht den Grundstein legen möchte, für eigene Experimente auf Kosten anderer. Es soll lediglich dazu dienen dem Leser ein Gefühl dafür zu geben, wie angegriffen wird und welche Schwachstellen es am eigenen PC, bzw. am eigenen Surfverhalten geben kann. Die Beschreibung erfolgt aus der Sicht des Angreifers.

3.1. Die IP des Opfers ermitteln

3.1.1. Mit Hilfe des AOL-Instant-Messanger

Seit dem AIM der Version 4 gibt es die Möglichkeit Bilder und andere Daten zu übertragen. Dazu muss man eine Direktverbindung herstellen. Falls der andere sich auch dazu bereit erklären sollte, diese Direktverbindung mit einem einzugehen, wird eine Verbindung über den Port 4443 aufgebaut. Und mit Hilfe eines Net-Monitors oder des Befehls *netstat* kann man nun die IP ermitteln. Geht der das Opfer nicht die Verbindung ein, kann man allerdings mit dem *netstat*-Befehl eine Verbindung mit dem Status *sys_sent* sehen, welche doch wieder die „heimliche“ AIM-Verbindung mit dem Opfer ist. AIM geht nämlich immer die Verbindung ein, wenn auch nicht offiziell.

3.1.2. Mit Hilfe des ICQ

Hier ist es ganz easy. Einfach eine Message abschicken und *netstat –a –n* eingeben und fertig.

3.1.3. Mit Hilfe des IRC

Einfach mit dem bekannten Befehl *\whois*.

3.1.4. sonstige Möglichkeiten

Auch wenn es wirklich trivial klingt, oft geht es mit simplen nachfragen. Wenn man sich ein wenig anstrengt und sich eine gute Story ausdenkt ... es gibt genug Leute, die darauf reinfallen. Man muss immer davon ausgehen, das am anderen Ende ein nur sehr unerfahrener Surfer sitzt, der nichts davon ahnt, das man mit der IP viel Schaden anrichten kann.

3.2. Angreifen

Erst einmal benötigt man ein sogenanntes IP Multitool (im Internet zu finden).

Als nächstes – nachdem nun die IP bekannt ist – lohnt es sich erst mal einen Portscan durchzuführen, so die ersten 150 Ports und dann noch die Trojaner-Ports (Listen dazu gibt's zu genüge im Internet).

Wenn dann ein schon vorhandener Trojaner gefunden wurde ist die Sache ja wirklich einfach. Man braucht sich dann nur noch den entsprechenden Client zu holen und los geht's.

Falls nicht, dann nach versucht man am besten über Telnet (Port 23) oder Netbios (Port 139) reinzukommen. Wie das dann funktioniert will ich an dieser Stelle nicht weiter beschreiben, weil es dazu ebenfalls wieder ausreichend Informationsmaterial im Internet gibt.

Falls das Opfer über eine Firewall verfügt, kann man meist mit einer einfachen DoS-Attacke auf den Rechner (innerhalb weniger Sekunden zig tausend Pings zum Beispiel). Die meisten Freeware- oder geklauten Firewalls brechen nach kurzer Zeit zusammen und geben den Rechner für ein paar Sekunden frei. Diese Zeit kann man nutzen um eine der oben genannten Verbindungen herzustellen. Häufig sind Firewalls bei unerfahrenen Home-Usern nur so eingestellt, das sie bei schon bestehenden Verbindungen keine Warnmeldung anzeigen.

3.3. Nachwort

Ich gehe jetzt nun nicht weiter und detaillierter auf dieses Thema ein, da dieser Text nur die Möglichkeiten eines Angriffs zum Zwecke des eigenen Schutzes darstellen soll. Im Internet gibt es genug Information über jede Art von Einbruch und über alle vorhandenen Sicherheitslöcher.

Carnivore - ein Raubtier im Internet?

Von Stefan Müller SS2001

Die Geschichte hat immer wieder gezeigt, daß die Regierungen dieser Welt kein High-Tech-Equipment benötigen, um ihre Bürger zu überwachen und auszuspionieren. Dennoch hat die Industrie neue Überwachungstechnologie entwickelt und Überwachung mit einer Tragweite ermöglicht, von der man in der Vergangenheit nicht mal zu träumen wagte. Wie Louis Brandeis Richter am Obersten Gerichtshof in den USA schon 1928 sagte: "Die größte Gefahr für die Freiheit lauert in hinterhältigen (wenn auch wohlgemeinten) Eingriffen von übereifrigen Menschen, denen die Langzeiteffekte und die anwachsenden Konsequenzen ihrer jeweiligen Handlungen entgehen."

Seit Jahrzehnten schnüffeln gewisse Organisationen das Privatleben des Weltbürgers aus und erstellen Profile. Wer heute ein Telefon, Fax oder Email benutzt, muß mit 24-stündiger Überwachung rechnen, wer Post verschickt kann sich darauf einstellen, daß auch diese nicht privat bleibt! Die Regierungen verschweigen grundsätzlich dieses Überwachungssystem, um Kritik zu verhindern. Doch beständige neue Maulkorbgesetzte gegen den Weltbürger zeigen an, was Regierungen tatsächlich planen!
Horrorvision à la George Orwell oder tatsächlich schon heute Realität?

Was genau ist Carnivore?

Der Begriff "Carnivore" entstammt aus der Biologie und bedeutet "Fleischfresser".
Carnivore ist ein sogenannter "Sniffer", ein "Lauscher", ein Set von Software Programmen, das den Netzwerkverkehr belauscht. Es ist Bestandteil eines Spionagepakets namens "Dragonware Suite". Außer Carnivore sind auch die Programme "Packeteer" und "Coolminer" Bestandteil der Suite. Mit diesen beiden Software-Tools werden die von Carnivore gesammelten Daten aufbereitet
Zum belauschten Netzwerkverkehr gehören also nicht nur Emails, sondern auch Unterhaltungen in Chaträumen, Webpages und andere Signale, die entweder von einer verdächtigen Person abgeschickt oder die an sie gerichtet wurden. Es ist in der Lage selbst größte Datenmengen, wie sie etwa beim täglichen Emailverkehr weltweit anfallen, in Echtzeit gezielt zu durchsuchen und verdächtige Post herauszufiltern um sie zur Strafverfolgung zu benutzen.
Das FBI betont aber, daß ihr Programm unter Berücksichtigung der Privatsphäre entwickelt worden ist und somit, anders als "herkömmliche" Sniffer, wesentlich feinere Filterregeln zuläßt. Es sucht nicht nach Schlüsselworten wie »Bombe« oder »Droge«. Es sucht nur mit Hilfe von bestimmten Kriterien, die das Gericht vorher erlauben muß. Es können also je nach Gerichtsbeschluß nur die Sender- und Empfängerdaten oder aber auch komplette Emails gespeichert werden. Somit setzt das FBI Carnivore vor allem dazu ein, Daten zu sammeln, um "Flüchtige, Drogendealer, Erpresser, Spione, Terroristen, Hacker, fremde Geheimdienste und sonstige Kriminelle" zu belasten, aber auch um illegale Glücksspiele und Geldwäsche aufzudecken.
Zur Anwendung kommt das Programm indem das FBI Carnivore beim Internet-Provider des Verdächtigen in einer Blackbox installiert und mit den Servern verbindet. Wird dann eine z.B. eine Email von oder an den Verdächtigen gefunden, dann wird der Text dieser Email kopiert und gespeichert. Täglich kommt dann ein FBI-Mitarbeiter und holt die Daten aus der Blackbox ab.
Also hat der Internet-Provider selbst keine Kontrolle über das System. Daraus ergibt sich dann das Problem, daß er nicht mehr kontrollieren kann, was abgehört wird. Überdies muß das System die gesamten über die Server laufenden Daten durchsuchen, um die herauszufischen, die zu einem Verdächtigen gehören. Dennoch beteuert das FBI: "Niemand braucht sich Sorgen zu machen, daß seine Emails kontrolliert würden, eben weil Carnivore nur nach vorgegeben Kriterien durchsucht".

Carnivore kann (je nach richterlichem Entscheid) in mehreren Stufen "abhören". Bei der einfachsten Form speichert das Programm lediglich Informationen darüber, mit wem ein Verdächtiger wann in Kontakt getreten ist. Dies entspricht in etwa der einfachsten Form des Lauschangriffs beim Telefon ("Pen Register" genannt). In der verdichteten Form (2. Stufe) registriert es welche Webseiten ein Verdächtiger aufruft und welche Chatrooms er besucht. Und schließlich in der 3. Stufe (intensivste Form) kann es nicht nur speichern, mit wem ein Verdächtiger kommuniziert, sondern auch, was er dabei sagt. Neben dem elektronischen Vorspann wird also auch der Inhalt des Datenpakets gespeichert.

Befürchtungen und Kritik zum Einsatz von Carnivore

Deshalb befürchten vor allem Verbraucherschutzverbände und Datenschützer wie ACLU (American Civil Liberties Union) oder EPIC (Electronic Privacy Information Centers) aber auch verschiedene Bürgerrechtsorganisationen und Abgeordnete, daß das System den verfassungsmäßig garantierten Schutz der Privatsphäre verletzte und dem FBI eine unkontrollierbare Lauschtätigkeit erlaube. Man könne, wenn das System einmal installiert ist, nicht mehr kontrollieren, was abgehört wird. Und überdies muß das System die gesamten über die Server laufenden Daten durchsuchen, um die herauszufischen, die zu einem Verdächtigen gehören. Das sei vergleichbar dem Fall, daß man alle Telefongespräche belauscht, um herauszufinden, ob es ein Telefongespräch gibt, daß man abhören müßte. Also könnte auch die elektronische Post unbescholtener Bürger kontrolliert werden.
Von der EPIC wird insbesondere kritisiert, daß Carnivore in der Lage ist, nicht nur den kompletten Emailverkehr zu scannen, der über den Server eines Providers läuft, sondern auch sämtliche Internet-Daten zu durchsuchen. Unter anderem wäre es dem FBI so möglich, herauszufinden, welche Webseiten von welchen Usern aufgesucht werden. Das stehe ganz und gar nicht im Einklang mit dem 4. Zusatzartikel (Electronic Communications Privacy Act) der Verfassung.
Ein weiteres Problem ergibt sich, da das Programm weder nach einer Autorisierung des Überwachers verlangt, noch festhält, wer das Programm wann und wie lange benutzt hat. Ihrer Meinung nach könnte das Schnüffelsystem so ohne weitere Kontrollinstanzen das Belauschen aller Kommunikationsvorgänge ermöglichen.
David Sobel vom EPIC sagte dazu: "Das Problem mit Carnivore ist, daß es dem FBI Zugriff zur Korrespondenz von Hunderten, wenn nicht Tausenden, unschuldigen Internet-Nutzern gibt. Es reicht [eben] nicht aus, wenn das FBI sagt: 'Traue uns, wir machen schon nichts Unerlaubtes.'" "[Denn] wenn es so einfach für das FBI ist, versehentlich zu viele Daten zu sammeln, kann man sich leicht vorstellen, wie einfach es für die Agenten ist, dies absichtlich zu tun", gibt er zu bedenken.

Prinzipiell könnte das FBI also auch ohne richterliche Abhörgenehmigung den Emailverkehr von beliebigen Menschen überwachen, wenn Carnivore erst einmal an die Computersysteme eines Providers angeschlossen ist.
Zwar werden noch immer meist die Telefonverbindungen abgehört, doch da das Abhören von Verdächtigen schon lange ein bewährtes Mittel in der Verbrechensbekämpfung ist, war es nur eine Frage der Zeit, wann dies auf den Bereich der Internetkommunikation ausgedehnt wird.
Zu den "gewaltigen, kaum ausgeschöpften Überwachungspotenzialen" gehören für die Kritiker auch, daß es Carnivore theoretisch auch möglich sei Paßwörter und Kreditkartennummern in seine Speicher zu filtern und daß es möglich ist, damit "Websites exakt so zu konstruieren, wie sie das zu überwachende Objekt während des Besuchs im Internet gesehen hat".
Sie befürchten in Carnivore die ersten Anzeichen für einen Überwachungsstaat.
Für sie ist Carnivore also tatsächlich ein gefährliches Raubtier, das im elektronischen Dschungel des Internets nach Fleisch sucht. Seine Beute sind digitale Indizien, mit denen leider nicht nur Straftäter dingfest gemacht werden können.

Forderungen der Bürgerrechtsorganisationen

So ist es nur natürlich, daß angesichts dieser Befürchtungen eine nicht unwesentliche Reihe von Forderungen seitens der Verbraucherschutzverbände, Datenschützer und Bürgerrechtsorganisationen gibt, um Carnivore so gut wie möglich zu entschärfen. Eine ihrer wichtigsten Forderungen ist es den Providern die Kontrolle über das System selbst zu geben, also die Hard - u. Software von Carnivore den Providern die es benötigen zugänglich machen. Die Provider sollen die Carnivore-Überwachung dann selbst durchführen und dabei sicherstellen, daß den Ermittlern nur der Datenverkehr der zu überwachenden Personen zugänglich wird.
Wenigstens solle Carnivore aber nur dann bei den Providern zum Einsatz kommen, wenn ein gerichtlicher Beschluß vorliegt.
Die zweite wichtige Forderung besteht in der Entwicklung von einheitlichen Standards in der Gestaltung von Überwachungs- und Abhörgesetzen. Die elektronische Kommunikation in den USA solle den gleichen Gesetzen unterworfen werden wie das Abhören von Telefonen.
Einen ähnlichen Vorschlag hat die Regierung bereits gemacht, nämlich die Vereinheitlichung der gesetzlichen Regelungen.
Dieser Vorschlag, so räumt auch ACLU ein, würde dem Richter immerhin größere Befugnisse gewähren. Bislang mußten nämlich Abhörgenehmigungen für die Internetkommunikation nur unterzeichnet werden. Nach diesem Vorschlag muß vor dem Abhören dem Richter das Vorliegen eines Verbrechens geschildert werden. Überdies können die Richter auch das Anlegen von Listen

überprüfen, in denen festgehalten wird, welche Telefonnummern von einem Anschluß angewählt und wann Gespräche geführt wurden. In einem Notfall allerdings, also wenn beispielsweise ein "Computerangriff" vorliegt, darf auch ohne richterliche Genehmigung der Täter zurückverfolgt werden. Wurde aber ohne Genehmigung abgehört, sollen die abgefangenen Emails nicht vor Gericht verwendet werden dürfen, was bislang nur für belauschte (Telefon-) Gespräche gilt.
Außerdem wurden auch Forderungen laut, daß das FBI den Quellcode offenlegt, um überprüfen zu können wozu Carnivore in der Lage ist.
Und vor dem Hintergrund, daß das Schnüffelsystem ohne weitere Kontrollinstanzen das Belauschen aller Kommunikationsvorgänge ermöglichen könnte, haben die Bürgerrechtsorganisationen in einem Schreiben an den US-Generalstaatsanwalt gefordert, das Carnivore-Modell neu zu überdenken.

Das FBI und sein Statement zu Carnivore

Natürlich versucht sich das FBI gegenüber allen diesen Forderungen, Kritiken und Befürchtungen zu rechtfertigen. So betonte z.B. FBI-Sprecher Paul Bresson, daß man die Mittel zum Abhören nur auf Emails erweitert habe, weil immer mehr Kommunikation vom Telefon auf Emails übergehe. Es sei lediglich eine "logische Erweiterung" der Überwachungstechnologie, die weder im Widerspruch zu den Gesetzen stehe noch eine Bedrohung des Datenschutzes darstelle. Außerdem rechtfertige die Zunahme von computergesteuerter Kriminalität der letzten Jahre den Einsatz von Carnivore.
Die sogenannten Blackboxes (in denen sich das Carnivore-System befindet) bei den Providern seien deswegen notwendig, damit niemand Beweise fälschen könne.
Und der Quelltext müsse geheim bleiben, damit niemand die Funktionsweise der zu Grunde liegenden Technologie herausfinden könne. Außerdem sei der Code Eigentum des FBI und durch eine Lizenz geschützt.
Außerdem bemühten sie sich zu beweisen, daß Carnivore weder "nach dem Zufallsprinzip durch Emails stöbere noch den gesamten Internet-Verkehr mitprotokollieren könne." "Carnivore hat nicht annähernd die Fähigkeiten, jeden mit einem Email-Account auszuspionieren", beteuerte das FBI.

Unerwartete Unterstützung in ihren Bemühungen erhielt das FBI dabei von Vinton Cerf. Der oft als "Vater des Internet" bezeichnete Wissenschaftler, Gründungsmitglied der Internet Society und Senior Vice President von MCI Worldcom verteidigte das umstrittene FBI-Abhörsystem Carnivore. Konkret wendet sich Cerf gegen die Forderung einiger Kritiker, die technischen Einzelheiten des Verfahrens aufzudecken. Ihr Argument, damit könne die Überwachungstätigkeit des FBI besser kontrolliert werden, lehnt er ab. "Die Carnivore Software in die Hand von Internet-Provider zu geben finde ich alarmierend, um offen zu sein", so Cerf. "Denn die Provider sind möglicherweise nicht so vertraut mit dem Strafrecht und haben somit vielleicht weniger Hemmungen als die Herrschaften vom FBI."
Auch die Kritik, Carnivore eröffne neue Möglichkeiten für Hacker, entkräftet Cerf. Er habe Einsicht erhalten in die technischen Grundlagen des Systems und bezeichnet es aufgrund seiner Prüfung als "very, very robust".
Und da Carnivore nur auf richterliche Anweisung hin zum Einsatz komme sei es fair. Es könne gesetzeskonform eingesetzt werden, da es so konfigurierbar sei, daß Absender und Empfänger von Emails erkennbar seien, der Inhalt der Nachricht jedoch nicht. Die Programmierer hätten in der Beziehung ganze Arbeit geleistet.
Carnivore, so Cerf, sei außerdem gar nicht in der Lage, den gesamten Emailverkehr im Internet mitzulesen, oder auch nur den bei einem einzelnen Internet-Provider. Das System sei vielmehr so ausgelegt, daß es aufgrund von wenigen vorher festgelegten Parametern entscheiden könne, ob ein bestimmtes Datenpaket für einen Überwachungsauftrag relevant sei oder nicht. Dieses könne nach erfolgter Entscheidung abgefangen und ausgewertet werden.

Bisheriger Einsatz von Carnivore

Nach eigenen Angaben des FBI sei Carnivore bislang bei 100 Fällen eingesetzt wurde. Die Fälle hätten vor allem mit dem "Schutz der Infrastruktur", mit der Verfolgung von Hackern, aber auch mit Terrorismusbekämpfung und Drogenhandel zu tun gehabt
Zwischen Oktober 1999 und August 2000 kam es 13 mal zum Einsatz, um Internet Datenverkehr aufzuzeichnen. Außerdem wurde es vorher als Testversion in 18 Monaten bei 25 Lauschangriffen eingesetzt.
Dies läßt durchaus die Vermutung zu daß Carnivore schon heute vielfach zum Einsatz kommt. Die Zahl der Ermittlungsaufträge beim FBI, bei denen es um die Online-Überwachung von Personen geht, soll sich alleine zwischen 1997 und 1999 um den Faktor 18,5 erhöht haben.

Erzwungene(?) Zusammenarbeit der Provider mit dem FBI

Das FBI ist nun vor das Problem gestellt, daß die Überwachung von IP-Datenverkehr von Personen, die Mitarbeit des Providers notwendig macht. Und das könnte sich schwierig gestalten. Denn neben EarthLink Inc., dem weltweit größten Internet-Provider, weigern sich auch viele andere Provider Carnivore in ihren Netzwerken installieren zu lassen. Es ist sogar ein Fall bekannt geworden, in dem ein Provider gegen den Einsatz von Carnivore in seinem Netzwerk klagte, dann aber per Gerichtsbeschluß zu Mitarbeit gezwungen wurde.
EarthLink erklärte zwar, dem FBI bei der Verbrechensbekämpfung auf jeden Fall helfen zu wollen, jedoch ohne dafür Carnivore in ihrem Netzwerk installieren zu müssen. Diese Befürchtung beruht auf einer Erfahrung, als Carnivore in Pasadena auf einem zentralen Site von EarthLink im Rahmen einer Fahndung installiert wurde und zunächst nicht kompatibel mit dem System des Providers war. Die ältere Version der Software, welche daraufhin installiert wurde, war zwar kompatibel, brachte aber unzählige Server mit Fernzugang zum Absturz.
Entgegen diesen Befürchtungen von Earthlink behauptet das FBI aber, daß das System auch nicht den gesamten Traffic eines Providers aufzeichnen oder irgendwie verfälschen könne. Ebenfalls sei es ihm auch nicht möglich, die Accounts von einzelnen Personen zu deaktivieren oder gar den Betrieb eines ganzen ISP lahm zu legen.

Ein Gutachten zum Einsatz von Carnivore

Aufgrund der nachdrücklichen Forderung nach Aufklärung über Carnivore seitens der Bürgerrechtsgruppierungen hat das US-Justizministerium (DoJ) im Juli 2000 grünes Licht gegeben und das Illinois Institute of Technology Research Institute (IITRI) in Chicago damit beauftragt "Licht ins Dunkel zu bringen."
Im Vorfeld lehnten jedoch etliche Universitäten, die das Justizministerium um eine Bewerbung gebeten hatte, unter dem Hinweis auf unzumutbare Vorgaben ab. Beispielsweise darf die untersuchende Organisation keine unabhängigen Kommentare abgeben. Darüber hinaus dürfen die Prüfer keine Programmteile unter die Lupe nehmen, die nicht vom Justizministerium freigegeben wurden. Laut MSNBC hat diese Vorgabe Generalstaatsanwältin Janet Reno den Vorwurf eingebracht, ihre Behörde strebe eine pauschale Generalamnestie für Carnivore an.

Der vorläufige Bericht des IITRI wurde Mitte November veröffentlicht – allerdings ohne Informationen über die Software-Struktur und die Funktionsprinzipien von Carnivore; diese wurden nur dem DoJ, nicht aber der Öffentlichkeit zugänglich gemacht.
In ihren Untersuchungen kamen die Experten vom IITRI zu dem Ergebnis, daß Carnivore tatsächlich nur die Daten aufzeichnet, die es nach einem entsprechenden gerichtlichen Beschluß aufzeichnen darf – wenn das System korrekt konfiguriert ist. Allerdings sei eine Fehlkonfiguration leicht möglich, wodurch sich das Volumen der gesammelten Daten enorm erhöhen könnte. Der Betrieb des Systems bringt nach Meinung der Experten auch keine Beeinträchtigung des Betriebs eines Providers mit sich.

Der IITRI-Bericht kritisiert aber unter anderem, daß in dem System keine Funktionen zur Überwachung des korrekten Betriebs eingebaut sind und daß die von Carnivore gesammelten Daten unzureichend gegen einen unberechtigten physischen Zugriff geschützt seien. Außerdem fanden die Computerspezialisten vom IITRI diverse Programmierfehler, über die sie das FBI in Kenntnis setzten.

Für das FBI sehr erfreulich ist die Bestätigung des IITRI, daß "Carnivore nicht annähernd ausreichende Kapazitäten hat, um nahezu jeden mit einer Email-Adresse auszuspionieren", wie dies von Bürgerrechtsgruppierungen vermutet worden war. Das System könne auch nicht den gesamten Datenverkehr eines Providers aufzeichnen oder irgendwie verfälschen. Ebenfalls sei es ihm auch nicht möglich, die Accounts von einzelnen Personen zu deaktivieren oder gar den Betrieb eines ganzen Providers lahm zu legen.

Eine Offenlegung des Quellcodes von Carnivore halten die Autoren des IITRI-Berichts zwar prinzipiell für wünschenswert, zum gegenwärtigen Zeitpunkt jedoch nicht für opportun. Die Software sei noch nicht ausgereift und die Offenlegungen des Quellcodes könnte Beeinträchtigungen der Funktion und der Sicherheit des Systems mit sich bringen.

Fachkreise und Sicherheitsexperten kritisierten allerdings das DoJ hätte dem IITRI nicht genügend Zeit eingeräumt, systematisch nach potentiellen Sicherheitslücken in Carnivore zu suchen. Standard-Schwachstellen wie Buffer-Overflows seien nicht systematisch geprüft worden und auch die Wechselwirkung mit verschiedenen Betriebssystemoberflächen hätte geprüft werden müssen: "Die

begrenzte Natur der bisherigen Analyse erlaubt keine Aussage darüber, ob Carnivore konsistent ist mit gesetzlichen Bestimmungen", urteilen die Sicherheitsfachleute in ihrem Papier und raten dem US-Justizministerium, eine Offenlegung der Carnivore-Quellen "ernsthaft in Erwägung zu ziehen". Außerdem kritisierten die Sicherheitsgurus, daß ein allmächtiger Administrator über das Carnivore-System wacht. Diese Konfiguration kann ihrer Ansicht nach schnell nach hinten losgehen, wenn ein unautorisierter User die Kontrolle übernimmt.

Aber auch aus anderen Ecken wurde Kritik an dem Bericht laut. So zeigt sich Dick Armey, Mehrheitsführer der Republikaner im US-Repräsentantenhaus, von dem positiven Tenor der Studie nicht überrascht. Das DoJ habe "die Experten und das Untersuchungsverfahren so ausgewählt, daß das Ergebnis bestmöglich ausfällt", polterte er. "Dieses bedeutende Problem bedarf einer wirklich unabhängigen Untersuchung, nicht einer Reinwaschung", fügte er hinzu.

Auch die Bürgerrechtsorganisationen Electronic Privacy Information Center (EPIC) und American Civil Liberties Union (ACLU) sind mit dem Bericht des IITRI und der Bewertung seiner Ergebnisse nicht zufrieden. Vor allem kritisierte David Sobel von EPIC, daß der Bericht nicht auf die prinzipiellen rechtlichen Probleme eingeht, die mit dem Einsatz des Schnüffeltools verbunden sind. Die EPIC fordert weiterhin einen vollständigen Einblick in alle Details des Carnivore-Systems. Die Organisation bereitet derzeit eine entsprechende Klage gegen das FBI und das DoJ vor. Außerdem fordert die EPIC Einsicht in den unzensierten Bericht des IITRI.

Schließlich ist auch die ACLU alles andere als zufrieden mit dem Bericht. "Was mich überrascht ist nicht die Tatsache, daß das Untersuchungsteam vor den Journalisten den Daumen über Carnivore hob, sondern daß sie erwarten, daß irgend jemand außerhalb der Regierung diesen Bericht ernst nimmt", sagte Barry Steinhardt von der ACLU. Ganz im Gegenteil zu den Aussagen des Berichts lägen Steinhardt Unterlagen vor, aus denen klar ersichtlich sei, daß Carnivore "zuverlässig den gesamten ungefilterten Traffic abfangen und speichern" könne.

Auch der auf Gerichtsbeschluß veröffentlichten und zunächst 750 Seiten umfassende Testbericht des FBI zum Probebetrieb von Carnivore wurde nicht vollständig veröffentlicht. Sofern die technischen Spezifikationen zu Hard- und Software nicht überhaupt aus "Sicherheitsgründen" zurück gehalten wurden, sind sie zu weiten Teilen eingeschwärzt, um die Verbreitung geheimer Informationen zu verhindern, so das FBI. Davon betroffen sind vor allem technische Details und damit jene Informationen, die Rückschlüsse auf die Leistungsfähigkeit des Gesamtsystems "DragonNet" zulassen würden.
Was der Testbericht über den Probebetrieb von "Carnivore" an harten Facts enthält, legt allerdings nahe, daß eine mögliche Veröffentlichung des Tests bereits beim Setup einkalkuliert war. Nach Angaben des FBI kam ein mit 300 MHz getakteter Pentium II [NT4 SP6] mit 384 MB RAM zum Einsatz. Bei einer "kümmerlichen" Festplattenkapazität von 1.19 Gigabyte mußten sich die FBI-Agenten mit Zip und Jaz-Laufwerken zur Speicherung der sicher gestellten Daten behelfen. Und das alles bei einem [offiziell zugegebenen] Budget von etwa 2,5 Millionen(!) Dollar für das Projekt - auch diese Zahlen sind nicht eingeschwärzt - für ein System, das aus dem Gesamtverkehr eines Internet-Providers sämtliche Datenpakete [Mail, WWW, FTP] einer Zielperson filtern soll.
Doch trotz dieser stellenweise massiven Zensur der Schriften will EPIC nun Anhaltspunkte haben, wonach Carnivore nicht nur in der Lage ist, gezielt den Emailverkehr einzelner Personen zu überwachen. Das System sei vielmehr dazu ausgerichtet, den gesamten Emailverkehr aller Anwender in den USA unter die Lupe zu nehmen. Die Emails nicht überwachter Personen könnten entgegen früherer Aussagen gesammelt und gespeichert werden.
Die der EPIC zur Zeit vorliegenden Text-Fragmente lassen immer noch einen gewissen Spielraum zu. Die strittige Passage besagt lediglich, daß es in einem Feldversuch möglich war, den IP-Verkehr ungefiltert – also ohne Beschränkung auf verdächtige Personen - auf einer Festplatte zu speichern. Ob das wirklich Aufgabe des Überwachungsssystems sein soll, bleibt fraglich. Doch schon das Vorhandensein der Möglichkeit läßt den Bürgerrechtlern die Haare zu Berge stehen. Und die Geheim-niskrämerei, mit der dieses System eingeführt wird, läßt eine Kontrolle kaum zu.
Auf insgesamt 160 der 750 Seiten wird der Source Code des Vorgänger-Programms "Omnivore" wiedergegeben, der unter Suns Solaris lief.
Der Rest der Dokumente beschäftigt sich ebenfalls hauptsächlich mit der Entstehungsgeschichte Carnivores. Demnach wurde das Projekt 1997 unter dem Namen "Omnivore" (Allesfresser) gestartet und wird seit dem Wechsel auf Windows-NT-Maschinen 1999 als "Fleischfresser" geführt.

Statistiken - wie der "gemeine" Bürger über Carnivore denkt

Wie der durchschnittliche Amerikaner über die Situation mit Carnivore denkt, wurde jetzt durch Untersuchungen verschiedener Umfrageinstitute deutlich.
Daß Surfer in puncto Datenschutz tatsächlich empfindlich sind, bestätigt eine aktuelle Untersuchung des Marktforschungsinstituts Ears and Eyes. Wie ZDNet berichtet, sind Surfer offenbar doch nicht so freimütig mit der Weitergabe persönlicher Daten wie bisher angenommen: "Surfern ist Datenschutz doch nicht egal". So "reagieren inzwischen neun von zehn Usern (89 Prozent) sehr mißtrauisch, wenn sie auf einer Internet-Site persönliche Angaben machen sollen." 64 Prozent ihre Antwort davon abhängig, welche Daten abgefragt werden, 45 Prozent beantworten persönliche Fragen nur, wenn auf der Seite deutlich gemacht wird, daß die Daten nicht an Dritte weiter gegeben werden, und weitere 45 Prozent hinterlassen ihre Angaben nur auf Sites, denen sie vertrauen (Mehrfachnennungen waren möglich).
Aber die zunehmende Besorgnis von US-Bürgern über kriminelle Machenschaften im Internet hat zu einem Sinneswandel gegenüber dem Email-Überwachungssystem Carnivore geführt. Angesichts der zunehmenden Internet-Kriminalität sieht die Mehrheit der Amerikaner die Mail-Überwachung als notwendiges Übel. Und Amerikaner, die bereits Bekanntschaft mit dem Carnivore-System gemacht haben, sprachen sich fast zur Hälfte für eine fortdauernde Anwendung des Schnüfflers aus. Darüber hinaus sprachen sich 62 Prozent dafür aus, daß ihr Land neue Datenschutz-Gesetze brauche.
In einer anderen Umfrage hatten sogar 73 Prozent der befragten Internet-Nutzer keine Bedenken mehr gegen ein Mitlesen von Emails auch von unverdächtigen Personen durch das FBI.

Gesetzliche Grundlagen zum Thema

Carnivore ist so umstritten, weil Amerika derzeit über kein Gesetz verfügt, das den digitalen Lauschangriff regelt. So gelten für Telefon, Kabelverbindungen oder andere Technologien bislang unterschiedliche gesetzliche Regelungen, die teilweise mit einander nicht vereinbar sind. Die verschiedenen Auffahrten auf die Datenautobahn unterliegen also unterschiedlichen Kontrollen. Beispielsweise unterliegt die Überwachung von jemandem, der über Modem und Telefonleitung mit dem Internet verbunden ist, den gleichen Regeln, wie sie für das Abhören von Telefonaten. Der Zugang über Kabelmodem wird dagegen nach den Regeln des im Jahre 1994 verabschiedeten "Cable Act" reguliert. Danach ist das Abhören digitaler Kommunikation nur erlaubt, nachdem der Abzuhörende informiert worden ist, was freilich für die FBI-Agenten wertlos ist. Für den Zugang über Funk gibt es dagegen überhaupt keine Regelung.
Bislang konnten die Sicherheitsbehörden, wie die New York Times schreibt, die Emailkommunikation mit einer nur geringen Kontrolle durch Richter überwachen.
Der Internet-Rechtsexperte Ulrich Sieber könnte sich allerdings eine Änderung dieser Kompetenzen vorstellen. Der Gesetzgeber müsse handeln, um der neuen Technik gerecht zu werden - immer mit Blick auf die Rechte des Einzelnen. Um die Verwertung von Verbindungsdaten zu sichern, wird beispielsweise das folgende Modell diskutiert: Die Polizei kann die Provider ohne richterlichen Beschluß anweisen, Daten eines Verdächtigen zu speichern, einsehen kann sie diese erst, nachdem ein Richter entschieden hat.
Allerdings gibt es auch jetzt schon sogenannte Einhaltungsbehörden (Law Enforcement Authoroties) wie etwa die dem FBI zugehörige Communications Assistance for Law Enforcements Act (CALEA) um die Befolgung der gesetzlichen Bestimmungen für die Datenüberwachung zu überprüfen, und dafür zu sorgen, daß Internet-Provider über ihre gesetzlichen Pflichten zur Sammlung und Weitergabe von Kundendaten aufgeklärt werden und die hierzu notwendige Infrastruktur unabhängig von ihren spezifischen Diensten bereitstellen.

Die Situation in Deutschland

In Deutschland wird das Programm bis jetzt noch nicht genutzt. Aber auch in Deutschland können Emails unter bestimmten Voraussetzungen aufgezeichnet werden. Ob das geltende Recht allerdings eine so extensive Durchsuchung auch unbeteiligter Emails durch ein System wie “Carnivore” zulassen würde, ist nach Einschätzung des Internet-Rechtsexperten Ulrich Sieber allerdings nicht zu klären, solange das FBI die genaue Funktionsweise im Dunkeln läßt.
Der Bundesnachrichtendienst (BND), der Entwicklungen im Ausland beobachtet, wertet zur Gefahrenabwehr ebenfalls Kommunikation nach Stichworten aus, allerdings in kleinerem Umfang. Dabei geht es zum Beispiel um den Handel mit Massenvernichtungswaffen. Nach einem Urteil des Bundesverfassungsgerichtes darf der BND Kommunikation auswerten, die über Satelliten läuft. Sprecherin Lydia Rauscher erklärt, daß noch zu bezweifeln sei, inwieweit die Kontrolle von Emails dem BND bei seiner Aufgabe helfe. Sie ergänzt: “Da gibt es sicher noch Handlungsbedarf.”

Die Sprecherin des Bundesbeauftragten für Datenschutz Helga Schumacher weiß zwar, daß Strafverfolger mehr wollen als jetzt erlaubt ist: “Die Polizei wünscht sich immer wieder eine strengere Linie.” Aber sie weist in diesem Zuge auf die Bestimmungen im Teledienste-Datenschutz-Gesetz hin. Danach darf der Internet-Provider personenbezogene Daten nur mit Einwilligung speichern.

Aber das Thema bleibt in der Diskussion: Im Februar haben das Bundeskriminalamt und Internet-Provider auf einer Tagung eine enge Zusammenarbeit beschlossen. Und die EU verhandelt über internationale Zusammenarbeit bei der Bekämpfung von Cyberkriminalität. Dennoch glaubt Schumacher, daß die hohen deutschen Datenschutz-Standards durch die Globalisierung nicht aufgeweicht werden.

Die Umbenennung von Carnivore

Zum Schluß läßt sich noch bemerken, das das FBI sein Email-Überwachungssystem umbenennt. Statt dem gefährlich klingenden Namen Carnivore (Fleischfresser) erhält der Datensammler das unverdächtige Kürzel DCS 1000, "Data Collection System 1000". Die Namensänderung wurde vom auch vom IITRI, welches das System im Auftrag des US-Justizministeriums überprüfte, vorgeschlagen. Der Name wecke zu viele negative Assoziationen und sollte daher geändert werden. Ein Sprecher des FBIs bestritt allerdings, daß die Namensänderung wegen der schlechten Publicity erfolgt. Außerdem wird die Namensänderung wird vom FBI mit einem Upgrade des Systems verbunden. Darüber ist aber bis jetzt leider nichts näheres bekannt geworden.

Resümee

Zuletzt läßt sich noch ein interessanter und diskusionswürdiger Fakt bemerken: US-Firmen sollen in Zukunft, ohne daß eine Genehmigung erforderlich ist, jedes Verschlüsselungsprodukt in die 15 Staaten der EU sowie nach Australien, Norwegen, Ungarn, Polen, Japan, Neuseeland und in die Schweiz und die Tschechische Republik exportieren dürfen.

John Podesta, Stabschef des Weißen Hauses, betonte, daß die Regierung weiterhin auf die Privatwirtschaft setzt, die verantwortlich für die Computersicherheit sei. Die Regierung verstehe sich als "Modellbürger", die weiterhin ein "Modell für die Informationssicherheit und "Datenschutzpraktiken" sein und mit der Privatwirtschaft eng zusammen arbeiten will. Bei allem Wandel sollen aber die grundlegenden Werte wie öffentliche Sicherheit, Schutz der Privatsphäre und bürgerliche Freiheiten gewahrt werden, während man die Lebensqualität der Amerikaner durch die Förderung des E-Commerce und den Abbau der digitalen Kluft verbessern wolle.

Wir dürfen also "gespannt" sein, wie sich die Situation in Zukunft in den USA und auch hier in Deutschland entwickelt.

Meine persönliche Ansicht zu diesem Thema ist eher zweigespalten. Auf der einen Seite finde ich es geradezu empörend, mit welcher Selbstverständlichkeit Organisationen wie das FBI und sogar Regierungen die Privatsphäre des "gemeinen" Bürgers unterwandern. Aber eigentlich kann man von solchen geheim arbeitenden Organisationen auch nichts anderes erwarten.
Andererseits läßt mich die Angelegenheit im Moment auch eher unberührt, wohl auch weil es mich bisher nicht unmittelbar betraf, d.h. ich bisher kein "sensibles" Material (nicht im negativen Sinne) zu verschicken hatte. Außerdem sind solche Methoden in Deutschland, wenigstens offiziell, nicht Gang und Gebe. Aber wenn sich der Trend in dieser Richtung weiterentwickelt, werde ich meinen Standpunkt auch noch mal überdenken müssen.

Das Echelon-System



Das Echelon-System ist ein globales Lauschsystem das von den UKUSA-Staaten (USA,UK,Australien, Neuseeland,..) genutzt und betrieben wird.
Echelon hat in den letzen 21/2 Jahren zu heftigen Diskussionen geführt, vor allem in Europa.
Grund war nicht nur seine Größe oder das dieses System über 50 Jahre geheim gehalten wurde, sondern weil man nicht 100%ig davon ausgehen kann, das dieses System nur zu Sicherheit der ganzen Welt dient oder ob nicht auch Wirtschaftsspionage damit betrieben wird.

Im Februar 2000 fand im Europäischen Parlament (erneut) eine Anhörung zum Thema „Die europäische Union und der Datenschutz“ statt. Durchgeführt wurde sie vom Ausschuß für Freiheiten und Rechte der Bürger. Sie stand unter besonderer Aufmerksamkeit, weil sie sich erstmals mit dem Echelon - Überwachungssystem befaßte. Als Grundlage der Anhörung dienten vier Studien, die vom Referat **STOA** (Scientific and Technological Options Assesment) der Generaldirektion für Forschung des Europäischen Parlaments in Auftrag gegeben wurden.
Darunter ein Bericht von **Duncan Campbell** über die elektronische Überwachung durch das Echelon-System . Besonders aktuell war in diesem Zusammenhang, dass geheime Vermerke der **NSA** veröffentlicht wurden und so erstmals die **Existenz des Echelon-Systems offiziell bestätigt** (http://www.heise.de/tp/deutsch/special/enfo/5721/1.html) wurde.

Duncan Campbell beschäftigte sich seit 1988 intensiv mit dem Thema Überwachungssysteme und schrieb einige Artikel (bei Telepolis : www.heise.de/tp/deutsch/special/ech/) über dieses System. Der sogenannte STOA-Bericht von 1998 findet man unter http://www.iptvreports.mcmail.com/stoa_cover.htm .

Im einem **STOA-Bericht von 1997** erwähnte Campbell erstmals das System zum Abhören kommerzieller Telekommunikationssatelliten (ECHELON) in einem offiziellen EU-Papier . Bei den darauf folgenden Diskussionen im Europa- Parlament wurde von den zuständigen Kommissaren noch behauptet, von der Existenz von ECHELON nichts gewußt zu haben. Der neue Bericht legte nun umfassende Materialien vor, in denen Geschichte und Arbeitsweise des ECHELON-Systems aufgezeigt werden.

Nicky Hager, ein neuseeländischer Autor, brachte 1996 ein Buch namens „Secret Power“ auf den Markt, in dem er über seine 6-jährige Forschungstätigkeit über eine neue Echelon-Station auf der neuseeländischen Insel Waihopai berichtete.

Die französische Regierung hatte als Konsequenz eine Kommission zur Überprüfung der Vorwürfe eingesetzt, und die Grünen im Europaparlament forderten darauf hin die Einrichtung eines parlamentarischen Untersuchungsausschusses, um den Behauptungen, die USA würden mit dem Echelon-System **Industriespionage** zugunsten amerikanischer Unternehmen betreiben, nachzugehen.
Es kam zu heftigen Diskussionen,vor allem weil von offizieller Seite die Existenz immer noch bestritten wurde.

Die Gruppe der Grünen/EFA im Europäischen Parlament präsentierten im März 2000 eine Liste mit 172 Unterschriften von Parlamentsmitgliedern aller politischen Gruppierungen, welche die Etablierung eines parlamentarischen Untersuchungsausschusses über Echelon forderten.
Damit sind genügend Unterschriften vorhanden, um eine Untersuchung über Echelon offiziell fordern zu können.

2 Wochen später entschieden die Präsidenten des Europäischen Parlaments, einen nichtständigen Ausschuss (1 Jahr) einzusetzen, der das Abhörsystem untersuchen solle.
Vor einigen Wochen ist ein vorläufiger Bericht des Untersuchungsausschuß vorgelegt worden, auf den später genauer eingegangen wird.
Zunächst wird aber genauer auf Echelon selber eingegangen.
Es gibt eine Menge Informationen zu diesem Thema, auf den nächsten Seiten wird das wichtigste zu Echelon dargelegt.
(Aufbau, die Funktionsweise und Geschichte von Echelon)

Quellen: 1) Telepolis-Magazin www.heise.de
2) STOA-Bericht von Duncan-Campbell http://www.iptvreports.mcmail.com/stoa_cover.htm

2. Das Echelon-System im Detail

(Quelle : „Inside Echelon“ von Duncan Campbell und andere Webseiten)

2.1 Was ist Echelon ?

Echelon (millitärisches Englisch: Staffelung) ist ein System, das von der US-amerikanischen **National Security Agency** (NSA) benutzt wird, um internationale Kommunikation abzuhören und zu verarbeiten, die über Kommunikations-Satelliten geleitet wird. Es ist Teil eines globalen Überwachungssystems, das bereits über 50 Jahre alt ist. Andere Teile desselben Systems fangen Nachrichten aus dem Internet, von Unterseekabeln und Funkübermittlungen ab. Sie nutzen die innerhalb von Botschaften installierten geheimen Lauschausrüstungen oder Satelliten in der Erdumlaufbahn, um Signale irgendwo auf der Erdoberfläche abzuhören. Zu dem System gehören Stationen, die von Großbritannien, Kanada, Australien und Neuseeland unterhalten werden - zusätzlich zu solchen, die von den Vereinigten Staaten betrieben werden. Obwohl die australischen und britischen Stationen dasselbe wie die Echelon-Stationen der USA tun, werden sie nicht notwendigerweise als Echelon-Stationen bezeichnet. Aber sie alle sind Teil desselben integrierten globalen Netzwerks, das dieselbe Ausrüstung und dieselben Methoden benutzt, um täglich verbotenerweise an Informationen und Aufklärungsmaterial aus Millionen von Nachrichten aus aller Welt zu gelangen.

Das System ist vorwiegend für nicht militärische Zwecke ausgelegt, nämlich neben der Beobachtung von terroristischen Aktivitäten und Waffenlieferungen zum Überwachen von Regierungen, Organisationen, Firmen und Individuen in fast jedem Land. Es betrifft fast jeden Menschen, der zwischen Ländern an irgendeinem Ort kommuniziert.
Abgehört wird jede Kommunikation, die über die Internationalen Telekommunikationssatelliten (Intelsats) und einige weitere Satelliten geht .
Es können aber auch Informationen belauscht werden die durch Kabel fließen, die auf dem Meeresboden liegen, die über das Internet übertragen werden oder Handygespräche.

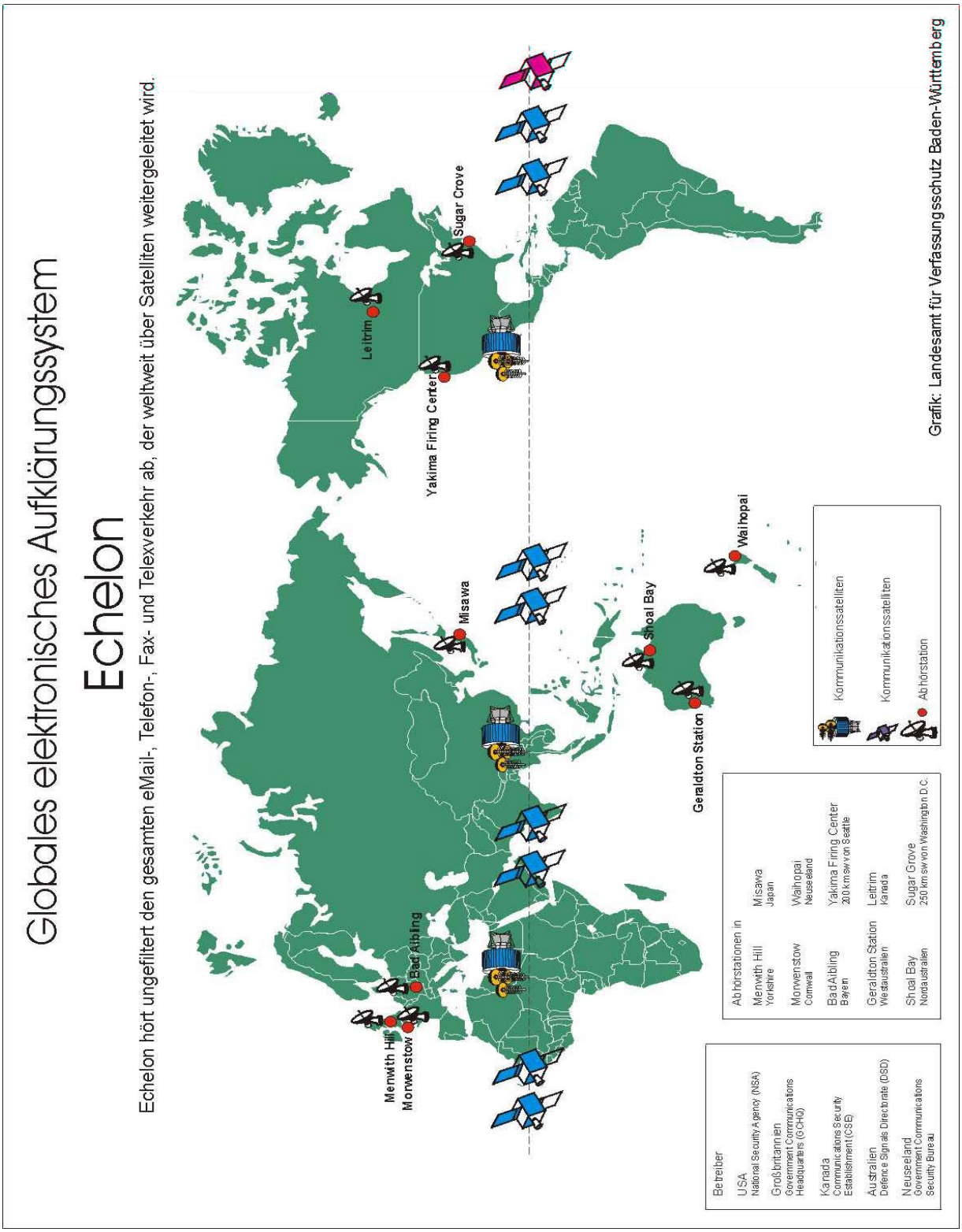
Somit ergibt sich die Hauptaufgabe von Echelon, Informationen abfangen und an andere (Teilnehmerstaaten der UKUSA) weiterzugeben.

Wobei sich natürlich die Frage stellt, ob diese Informationen auch zu amerikanischen Firma gelangt sind (siehe 4. Wirtschaftsspionage ?).

Dieser Vorgang erfolgt in 3 Schritten :

a) Sammlung aller nur möglicher Informationen
b) Ihre Analyse und die Suche nach dem entsprechend Kontext
c) die Verteilung der Zuständigkeiten

2.2 Das Netzwerk

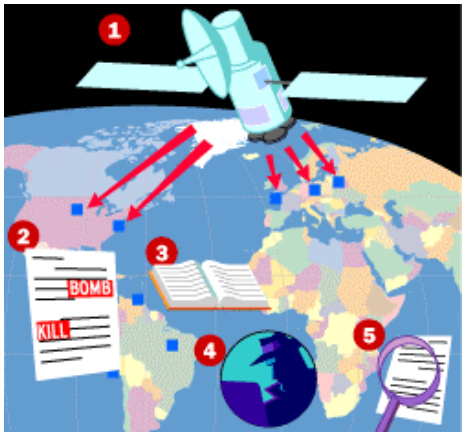


Die Zentrale von Echelon ist in Fort Meade (Maryland/USA) und ist über ein Netzwerk verbunden mit 7 terrestrische Abhörstationen (ingesamt 120 Abhörstationen)

[Menwith Hill (GB), Morwenstow (GB), Geraldton (Australien),Waihopai (Neuseeland), Yakima (USA),Sugar Grove (USA), Bad Aibling (Deutschland)] .

Diese sind über Unterseekabel und Satelliten (größtenteils amerikanische und britische Militärkommunikationssatelliten) miteinander verbunden.
Das Netzwerk wurde Ende der 70iger Jahre massiv erweitert. Grund war die Einführung kostengünstiger, breitbandiger, internationaler Kommunikation.
Dies führte dazu, dass das Echelon das zu dieser Zeit größte WAN war das bis dahin existierte.
Das WAN ist nach denselben Prinzipien wie das Internet (TCP/IP) angelegt und ermöglicht allen Abhörstationen den Zugang zum zentralen Computersystem der NSA, bekannt als (eng.) "Platform".
Das Herz jeder Abhörstation ist das sogenannte „Dictionary“.
Jede Echelon- Station enthält ein "Dictionary". Die Dictionary-Computer untersuchen den empfangenen Daten und extrahieren, was den Interessenprofilen entspricht, für Berichte und weitere Analysen. In einem gewissen Sinn besteht die Hauptaufgabe der Dictionary-Computer darin, den größten Teil der abgehörten Informationen wegzuwerfen.

2.3 Funktionsweise



1. Das Echelon-System fängt über die Satelliten den größten Teil der Kommunikation von Regierungen, Wirtschaftsunternehmen und Privatleute ab.
   (Fax, Telefongespräche und E-Mails)
2. Es ist möglich speziell nach Daten mit bestimmten Keywords (z.B. Namen von Unternehmen, Ländern usw.) zu suchen
3. Die Suche erfolgt durch das Dictionary, einem speziellen Computer, der die Keywords enthält. Er siebt alle empfangenen Daten und die „Dokumente“ die nicht eines der Keywords enthalten, werden rausgeschmissen.
4. Mitarbeiter des Geheimdienstes können sich an einem Echelon-PC einloggen, und sich die gefilterten Daten anschauen.
5. Die Mitarbeiter filtern erneut und verwenden nur das was sie für spätere Ermittlungen benötigen. Die übriggebliebenen Daten werden an die anderen Stationen weitergegeben

2.4 Abhörmöglichkeiten

2.4.1 Das Abhören von Funk und mobilen Telefongesprächen

Drahtlos übertragene Signale können allgemein per „Fernabfrage“ abgehört werden.
Echelon besitzt mehrere Stationen, die Kurzwellen-Übertragungen mitschneiden und ihren Ursprung genau feststellen können.
Radiosignale werden, obwohl sie nach mehrere hundert Kilometern durch die Erdkrümmung abgeschirmt werden, mitgeschnitten werden.
Mit Hilfe von Satelliten ist Echelon in der Lage Mobiltelefone oder Mikrowellen-Verbindungen direkt abzuhören.
Möglich wird dies durch Querschläger, die in den Weltraum verschwinden, und werden dort von Satelliten aufgefanngen.

2.4.2 Bodenstationen und Satelliten

Hauptsächlich werden mit Hilfe der Bodenstationen von Echelon in Großbritannien und den USA Daten zwischen Intelsat-Kommunikations-Satelliten angezapft.
Außerdem schneiden Hilfsstationen, die nahe an den Bodenstationen der Intelsat-Satelliten liegen, deren Mikrowellen-Abstrahlungen mit.
Überall dort, wo Mirkrowellen-Strahlung kontzentriert auftritt (in Städten) wird ebenfalls spioniert.

Man vermutet sogar, das andere Satelliten-Systeme Komponenten der NSA enthalten, so daß die Daten direkt von dort aus an die Bodenstationen gesandt werden!

2.4.3 Das Anzapfen von Kabeln

Das Anzapfen von Kabeln funktioniert nicht so unaffällig wie bei Funkfrequenzen, aber es ist durchaus an der Tagesordnung.
Beispielsweise werden in GBR internationale Telefongespräche, Faxe oder Daten an Kabelverzweigungen mitgeschnitten.

Auch das Anzapfen von Unterseekabeln durch U-Boote ist möglich.

3. Geschichte

(Quellen : Telepolisartikel „Inside Echelon“ und „Echelon Chronology“ von Duncan Campbell)

Im Zweiten Weltkrieg hatten mehrere dutzend fortschrittliche Nationen Netzwerke zur elektronischen Fernmeldeaufklärung.

Zum Beispiel **Großbritannien** GCHQ verfügte über ein weitreichendes Netzwerk von Außenposten mit Sationen in Großbritannien selber und im ganzen damaligen Empire verteilt
(Bermuda, die Ascension-Inseln, Zypern, Gibraltar, Irak, Singapur und Hongkong)

Das System basiert auf der "UKUSA-Vereinbarung" von **1947**, wonach sich das britische und US-amerikanische System miteinander vereinten. Später schlossen sich die Netzwerke der drei britischen Commonwealth-Länder Kanada, Australien und Neuseeland an.
Es wurden Hauptquatiere eingerichtet. Die USA unterhalten ein spezielles US-Verbindungsbüro (SUSLO) in London und Cheltenham, während ein Vertreter des speziellen britischen Verbindungsbüros (SUKLO) des GCHQ seine Büros innerhalb des NSA-Hauptquartiers in Fort Mead, zwischen Washington und Baltimore, unterhält.

UKUSA-Vereinbarung = fünf englischsprachigen Länder teilten sich die Verantwortung für die Überwachung auf verschiedene Teile des Globus auf.
Großbritannien : Afrika, Europa sowie Richtung Osten bis zum Ural;
Kanada : nördliche Breitengrade und Polarregionen
Australien : Ozeanien
Die Vereinbarung schrieb gemeinsame Vorgehensweisen, Ziele, Ausrüstung und Methoden vor, die die Abhöreinrichtungen nutzen sollten. Dazu gehörten auch internationale Regeln für die Sicherheit der elektronischen Fernmeldeaufklärung.

1960 bestand das Netzwerk aus Tausenden von ständig betriebenen Abhör-Standorten.

Mitte der 60er-Jahre wurden viele Stationen mit gigantischen Antennensystemen zur Überwachung des Hochfrequenzfunkverkehrs errichtet. Sie waren auch in der Lage, die Position eines Senders zu lokalisieren .

1964 International Telecommunications Satellite Consortium formed to launch civil communications satellites (comsats)

1965 Abhören von Funknachrichten des Warschauerpaktes und des kommerziell betriebenen Funkstreckenverkehrs zwischen den großen europäischen Städten

1967 First comsat interception station planned at Morwenstow, Cornwall, England

Anfang 70iger Jahre Einführung von Listen mit Schlüsselwörtern
Viele prominente Amerikaner wurden der Liste beigefügt (Jane Fonda, Dr. Benjamin Spock ...)
Das Durchsuchen der Daten wurde allmählich durch automatisierte Computersysteme ersetzt.
Die NSA und die CIA entdeckten, dass die elektronische Fernmeldeaufklärung im Weltraum weit effektiver und produktiver ist

1970 First comsat interception station in operation at Morwenstow

1971 Second comsat interception station in operation at Yakima, Washington, USA

1976 Einrichtung einer speziellen neuen zivilen Einheit in Chicksands zum Abhören der diplomatischen und zivilen Kommunikation durch die NSA

Ende der 70er Jahre war Menwith Hill in Mittelengland eine der Hauptstationen für die Verarbeitung von abgehörter Weltraum-Kommunikation

80er Jahre entwickelte die NSA den schnellen Datenfinder-Mikroprozessor

1981 Echelon II database in operation at Menwith Hill, Yorkshire, England; expansion of Echelon system planned

1982 Ladylove comsat interception station in operation at Misawa, Honshu, Japan

Mitte der 80er Jahre massive globale Erweiterung des Echelon-Systems
und der Telekommunikationsverkehr, der von den Dictionary-Computern rund um die Welt erfasst wurde, wurde mit einer großen Bandbreite von Spezifikationen für den nonverbalen Verkehr durchsiebt

1984 schlossen sich Australien, Kanada und Neuseeland den USA und Großbritannien beim Betreiben von Comsat-Abhörstationen an.

1985 Canadian comsat interception station in operation at Leitrim, Ontario, Canada

1986 Global expansion of Echelon system planned by UKUSA treaty partners

1988 Existence of Echelon interception system revealed for the first time in British magazine New Statesman

1989-91 New comsat interception stations start operation in Australia and New Zealand

1990 zeigten Satellitenaufnahmen vier Satellitenschüsseln in Sugar Grove. Eine Untersuchung vom Boden aus ergab im November 1998, dass diese inzwischen auf neun erweitert worden waren

1996 New Zealand researcher Nicky Hager publishes “Secret Power”, describing the Echelon system

1998 European Parliament publishes report on the “Technology of Political Control”, mentioning the findings of “Secret Power”

May 1998 Documents released to the National Security Archive in Washington confirm the existence of Echelon satellite interception stations, run by the U.S. military

March 1999 Martin Brady, director of the Australian signals intelligence organisation DSD, confirms that Australia takes part in UKUSA intelligence sharing system

May 1999 European Parliament published “Interception Capabilities 2000” (IC2000) report describing Echelon and other parts of the global interception system

February 2000 IC2000 report presented to European Parliament March 2000 Former CIA director James Woolsey confirms that U.S. intelligence uses interception systems and keyword searches to monitor European businesses

July 2000 European Parliament vote to set up temporary committee on the “Echelon interception system”

October 2000 French Assemblee Nationale publishes report on Echelon and affirms that “Echelon exists”

December 2000 Echelon Committee of European Parliament commissions further studies (IC2001) on the use of interception systems

January 2001 Dutch Parliament report on Echelon affirms that “Echelon exists”

February 2001 EU official Desmond Perkins tells the Echelon Committee that he gave samples of EU codes to NSA for testing, adding “the Americans read everything”

April 2001 New Zealand author Nicky Hager gives evidence to Echelon committee

14 May 2001 US government cancels all meetings with the Echelon Committee during their visit to Washington “at the last minute”.

23 May 2001 Draft final report of Echelon Committee leaked and published

4. Wirtschaftspionage ?

Wie bereits am Anfang erwähnt, kam es nach bekanntwerden der Details zu Echelon zu heftigen Diskussionen.
Hauptgrund war nicht alleine nur die Tatsache, das so ein System existiert, sondern auch, weil man nicht ausschließen konnte, daß die abgefangenen Daten zu Firmen der Echelon-Mitgliedsstaaten gelangten.

Zum Beispiel bei einem geplatzten Airbus-Geschäft mit Saudi-Arabien in Höhe von gut 10 Mrd. Dollar vermutet man, das Echelon der Grund war. Damals bekam schließlich McDonnel-Douglas den Zuschlag, weil sie die Gebotssumme von Airbus kannten.

Natürlich sind dies alles Vermutungen.
Offiziell gibt man bei der CIA (CIA-Direktor James Woolsey) zu, amerikanische Unternehmen viele Milliarden Dollar verschafft zu haben. Man weist aber die Anschuldigungen der Wirtschaftsspionage entschieden zurück.
Statt dessen gibt man zu, daß man ausländische Unternehmen wegen Bestechung überwacht, und falls ein Verdacht auftaucht, man mit Sanktionen droht, wenn das Geschäft trotzdem abgewickelt wird. Wenn das europäische Land wirtschaftlich oder anderweitig von den USA abhängig ist , wird der Vertrag natürlich nicht geschlossen.

Nach Informationen von MSNBC kam es schon oft zu so einer Mithilfe der CIA.

Beispiele:

- Boeing beim Verkauf von 747-Flugzeugen an Saudi-Arabien
- Raytheon beim Verkauf eines Überwachungssystems an Brasilien
- Hughes Network Systems beim Verkauf eines Telekommunikationssystems an Indonesien

Aus technischer Sicht ist die Wirtschaftsspionage auf jeden Fall möglich, da oft die Kommunikation unverschlüsselt über Satelliten erfolgt.
Dazu gleich mehr.

5. Alles nur Übertrieben

(Quellen: Interview Telepolis mit Gerhard Schmid einem Ausschußmitarbeiter)

Am 18.Mai 2001 wurde der mit Spannung erwartete „vorläufige“ Bericht über das Abhörsystem vom nichtständigen Ausschuß vorgelegt.
(zu finden unter : Link!!)

Der etwa 120 Seiten lange Bericht informiert ausführlich über das Geheimdienste (Tätigkeiten und Arbeitsweise), genutzte Abhörmöglichkeiten, Satellitensysteme und welche Möglichkeiten man aus technischer Sicht hat, die Satellitenkommunikation abzuhören.
Außerdem wird auf die Rechtslage von Echelon eingegangen.

Einige Wochen bevor dieser Bericht erschien, äußerte sich bereits der Ausschußberichterstatter Gerhard Schmid zu diesem Thema.

Im groben ist man zu dem Ergebnis gekommen, das dieses System Echelon existiert, wenn gleich unter einem anderen Namen, aber man die Fähigkeiten dieses Systems etwas überschätzt.

Unklar ist geblieben, ob damit Wirtschaftspionage betrieben wird.

Aus dem Bericht ist auch klar zu entnehmen das man (fast) keine rechtliche Möglichkeit hat gegen dieses System vorzugehen.

Zum Inhalt :

Der Ausschuß hat nur wenig neue Erkenntnisse gebracht, da man hauptsächlich mit Indizienbeweisen arbeiten mußte.
Man hat keine Details über das System selber, aber man hatte mit Hilfe von Experten die Möglichkeit Schlußfolgerungen zu ziehen, aufgrund von Kenntnissen aus dem Bereich der Nachrichten- und Kommunikationstechniken.
Man traf sich mit Regierungsvertretern von GBR, Frankreich und den USA.
Diese gaben nur wenig paar Auskunft, in den USA wurde sogar den Delegierten des UA s die Tür vor der Nase zugeschlagen.

<u>Abhören von Satellitenverbindungen ?</u>

Vorraussetzung für das Abhören ist der richtige Standort. Befindet man sich im Ausleuchtradius des abzuhörenden Satelliten , also im Bereich des sogenannten footprints, ist es mit einer entsprechenden Schüssel möglich die Verbindungen abzuhören, wenn keine entsprechende Verschlüsselung erfolgt. Wirtschaftskommunikation, also Videoconferencing erfolgt oft unverschlüsselt.

Betroffen können sein beispielsweise die INTELSAT Satelliten oder einfache nur regionale wie ARABSAT.

Das Abhören von Handy-Gesprächen über Satelliten ist nach Expertenmeinung so gut wie unmöglich.

<u>Grund 1:</u>
Der Mobilfunk in Europa ist über Funkzellen, die jeweils 30 Kilometer weit reichen, organisiert. Die verschiedenen Gesprächskanäle werden über verschiedene Frequenzen abgewickelt.
Wenn Sie sich an einem Ort einwählen, benutzt die Funkzelle eine bestimmte Frequenz. Die benachbarten Funkzellen benutzen jedoch andere Frequenzen. Nach einer gewissen Entfernung wiederholen sich jedoch wieder die benutzten Frequenzen. Bei einer Abstrahlung in den Weltraum mischen sich diese Frequenzen und Sie können sie nicht mehr einzeln auseinander halten.

<u>Grund 2:</u>
Die Sendestärken.

Abhören einer Richtfunkstrecke?

Mit Hilfe eines geostationären Satelliten kann man im Weltraum dann eine Richtfunkstrecke abhören, wenn er auf der Verlängerung der Strecke ins All sitzt. So ein Aufwand ist jedoch nur für militärische Richtfunkstrecken denkbar, über die zum Beispiel wesentliche Befehle für U-Boote oder Raketen übermittelt werden.

Abhören Unterwasserkabeln und Glasfaser-Technik?

Das Anzapfen von Unterwasserkabeln spielt kaum eine Rolle. Es wurde von den USA mit Kupferkoaxialkabeln gemacht, über die unverschlüsselte Kommunikation zu den U-Boothäfen im russischen Eismeer gelaufen ist. Mit Hilfe einer Spule, die man mit einem U-Boot neben das Kabel legt, kann man bei der Kupferaxialtechnik auf elektromagnetischem Wege das Kabel nach dem Transformatorprinzip anzapfen.
Bei Glasfasern funktioniert das nicht. Bei den alten Glasfaserkabeln musste in bestimmten Abständen in das Kabel ein Verstärker eingebaut werden, der die Lichtwellen in Strom und dann wieder in Lichtwellen umwandelte. Das kann man theoretisch induktiv anzapfen. Das macht nur Sinn, wenn Sie sich direkt mit einem U-Boot daneben setzen und dort auch auswerten.

Rechtsgrundlagen:
Nach dem EU-Recht, ergibt sich nur eine Verletzung, wenn **ein Mitgliedsland** ein Echelon-ähnliches System zur Wirtschaftsspionage missbraucht.
Ein Belauschen der Kommunikation europäischer Bürger "ohne Gewährleistung der Einhaltung des Verhältnismäßigkeitsprinzips" würde das Grundrecht auf Privatsphäre (Art. 8 der Europäischen Menschenrechtskonvention) verletzen.
Aber dennoch, rechtlich lässt sich gegen ein Abhören von Privat- oder Geschäftspersonen nur im Rahmen der Menschenrechtskonvention vorgehen, die zwar alle Menschen einschließt, also auch für Nicht-EU-Bürger gilt, aber viele Ausnahmen kennt: gelauscht werden darf in Übereinstimmung mit den gesetzlichen Rahmenbedingungen im Interesse der nationalen Sicherheit, der öffentlichen Sicherheit oder des wirtschaftlichen Wohlergehens des Landes, zur Abwehr von Unordnung oder Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten von Anderen.

Fazit: Nur die Regierungen der einzelnen Staaten können etwas dagegen tun, in dem sie spezielle Gesetze verabschieden oder die Geheimdienste kontrollieren.
Wichtig ist auch eine Verstärkung der Verschlüsselung von Daten!!

6. Contra Echelon

(Quelle : http://www.heise.de/tp/deutsch/special/ech/6768/1.html)

In einigen Staaten, vor allem in den USA, hat sich im Laufe der Zeit ein Netzwerk von Überwachungsgegnern entwickelt, welche man auch mit dem Namen „Cyber-Rights-Activists“ etikettiert.
Diese setzen sich vor allem für die Bürgerrechte in der Informationsgesellschaft und gegen eine Ausweitung der Überwachung ein.
Früher noch überwiegen Juristen, heute sind eher IT-Fachleute Mitglieder dieses Netzwerkes.

Hier nun einige der wichtigsten Gruppen/Organisationen.

USA

Hier haben Organisationen die sich vor allem für die Bürgerrechte einsetzen eine lange Tradition.
Die größte und bekannteste ist die 1920 gegründete **ACLU** (Amercian Civil Liberties Union).
Früher setzte sich diese Gruppe eher für Redefreiheit und gegen Rassendikriminierung ein, heute mehr und mehr gegen die Überwachung im Internet.

Aktuelle Themen der ACLU :

- Überwachungsbefugnisse des FBI
- ECHELON
- Datenschutz und Meinungsfreiheit im Internet

Gemeinsam mit der **CPSR** (Computer Professionals for Social Responsibility) klagte sie erfolgreich gegen den CDA (Communication Decancy Act) also Einschränkung der Meinungsfreiheit im Internet.
1983 als Verein gegründet ist die älteste von IT-Experten und Wissenschaftlern gegründete Organisation.
Beraten Parlamente auf Landes- und Bundesebene.

1994 wurde aus dem Washingtoner Büro die **EPIC** (Electronis Privacy Information Center).
Gemeinsam mit der Trägerschaft „ Fund for Constitutional Government“ wurde eine **Forschungstelle** zum Thema Privatheit und Bürgerrechte in der Informationsgesellschaft gebildet.

Die Gründung der **GILC** (Global Internet Liberty Campaign) 1996 führte zu Vernetzung der in allen Ländern bestehenden gleichgesinnten Organisationen.
Verbesserung der organisierten internationalen Kontakte, was zu großen Erfolgen führte im Kampf gegen die Überwachnung im Internet.

GBR

Auch hier gibt es verschiedene Cyber-Right-Groups.
Eine davon ist **Statewatch .**
Themen:

- Überwachung
- Asyl und Flüchtlinge
- Kampf gegen Rassismus

Deutschland

In Deutschland gibt es auch vereinzelt Gruppen die sich gegen eine Zunehmende Überwachung im Internet stark mache.

Die FifF („Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung") e.V,. ist ein Verein der 1984 nach dem Vorbild CPSR gegründet.

Sie ist eine Schwesterorganisation und tritt setzt sich allgemein mit den Auswirkungen der IT-Technik auseinander.
Sie ist sehr aktiv, berät den Bundestag und das Europaparlament.

Oft arbeitet die FifF zusammen mit der deutschen Vereinigung für Datenschutz (DVD), die 1977 gegründet wurde.

Die bekannteste Gruppe von IT-Fachleuten dürfte in Deutschland der 1986 gegründete "Chaos Computer Club" (CCC) sein.

7. Informationsquellen / Links

Jede dieser eben erwähnten Gruppen /Organisationen sind im Internet vertreten.

Usa
www.aclu.org
www.cpsr.org
www.epic.org
www.gilc.org
www.eff.org

GBR
www.statewatch.org
www.privacyinternational.org

GER

www.ccc.de

Darüber hinaus gibt sehr viel andere Links zum Thema Echelon oder Überwachung im Internet.
Hier sind einige mir aufgefallene Seiten:

www.echelonwatch.org

Auf dieser Seite findet man sehr viel weitere interessante Links zum Thema!

Die Informationen in diesem Bericht stammen hauptsächlich von der Internetzeitschrift TELEPOLIS, die man unter www.heise.de findet.
Hier gibt einen speziellen Bereich, das Echelon-Archiv, wo man sehr viele Artikel über Echelon fnden kann.

Wer sich den Ausschußbericht bzw. den vorläufigen Entwurf durchlesen will , hier die Adresse :
http://www.europarl.eu.int/tempcom/echelon/prechelon_en.htm