Die bedrohte Sicherheit von Informationsnetzen*

Hannes Federrath

30. November 2001

1 Einführung

Mit der zunehmenden Abhängigkeit unserer Informationsgesellschaft von schnellen Kommunikationsverbindungen über Internet und Telefon wächst auch deren Verletzlichkeit. In nahezu allen Lebensbereichen ist Informationstechnologie (IT) heute anzutreffen. Alle größeren technischen Systeme nutzen informationstechnische Ausstattungen. Selbst jedes moderne Fahrzeug ist heute mit mehreren Mikrorechnern ausgerüstet.

Die aus dieser Abhängigkeit von IT entstehenden Bedrohungen hängen vom Bereich ab und von der Wichtigkeit der verarbeiteten Daten. Bisher wurden manche möglichen Angriffe auf Kommunikationsnetze in der Realität alleine deshalb ausgeschlossen, weil niemand das Vorhandensein einer Motivation, den Angriff tatsächlich durchzuführen, für wahrscheinlich hielt. Mit den Terroranschlägen in den USA haben sich auch diese Wahrscheinlichkeiten geändert. Die Hauptbedrohungen für unsere Netze gehen momentan aus von mangelhafter Software und daraus resultierenden Denial-of-Service Angriffen, Datenspionage und Viren, Würmern und trojanischen Pferden. Softwarefehler werden oft erst spät, manchmal zu spät, entdeckt und können zu hohen Schäden führen.

Bisher ging man meistens davon aus, dass Angreifer versuchen werden, nicht gefasst zu werden, die Motivation im Verschaffen von Vorteilen (z.B. finanzielle) lag oder es den Angreifern darauf ankam, durch große Schäden großen „Ruhm“ innerhalb ihrer Subkultur zu erlangen. An diesen Motivationen hat sich nichts geändert; hinzugekommen sind jedoch Angreifer, die keine Angst davor haben, selbst zu Opfern ihrer Angriffe zu werden, die politische oder religiöse Ziele verfolgen und möglicherweise subtile (anstelle von großflächigen, ungezielten) Schäden in bestimmten Sektoren (z.B. Informationsnetze der westlichen Finanzsysteme) oder kritischen Infrastrukturen verursachen wollen.

Dieter Kaundinya, Abteilungsleiter für internationalen Terrorismus des deutschen Auslandsgeheimdienstes, unterstrich auf der Herbsttagung des Bundeskriminalamtes in Wiesbaden diese Bedrohung: „Zunächst waren es Angriffe vom Boden, dann vom Wasser und dann aus der Luft. Das nächste wäre vielleicht der Cyberwar, eine Attacke, mit der die Daten- und Kommunikationsverbindungen der modernen Gesellschaft getroffen werden sollen.“ [1]

Mit langjähriger und guter Vorbereitung wäre es Cyber-Terroristen möglich, die westlichen Finanzmärkte mit Hilfe von Computerviren und trojanischen Pferden der-

*Eine leicht gekürzte Fassung dieses Aufsatzes ist in *Felicitas von Aretin, Bernd Wannenmacher (Hrsg.): „Weltlage – Der 11. September, die Politik und die Kulturen“, Verlag Leske + Budrich, Opladen 2002, 163-173.* erschienen.

art zu stören, dass ernsthafte (auch dauerhafte) Schäden nicht ausgeschlossen wären. Vermutlich würden beispielsweise Börsen nicht mittels Denial-of-Service-Angriffen gestört, vielmehr könnten Hacker die Transaktionen unauffällig manipulieren und das Finanzsystem subtil durcheinander bringen.

Bedauerlicherweise sind die Schutzmöglichkeiten gegen solche Attacken momentan noch sehr begrenzt: Heterogenität, d.h. keine Monokultur im Software- und Hardwarebereich, Offenlegen der Software (Open Source), um Programmierfehler besser zu finden, Einsatz von Verschlüsselungsverfahren zur Vermeidung von unberechtigtem Mitlesen und Datenspionage, Vermeidung von Abhängigkeiten von einem einzigen Kommunikationsnetz und damit Aufrechterhalten alternativer, diversitärer Kommunikationsinfrastrukturen.

Dieser Aufsatz ist folgendermaßen aufgebaut: Zunächst wird eine kurze Systematisierung der Bedrohungen gegeben (Abschnitt 2). Anschließend sollen konkrete Angriffe als Fallbeispiele für die bedrohte Sicherheit von Informationsnetzen dienen: Der Abschnitt 3 beschäftigt sich mit Denial-of-Service Angriffen im Internet, in Abschnitt 4 wird auf Bedrohungen durch mangelhafte Software eingegangen, im Abschnitt 5 werden die Bedrohungen durch Computerviren, Würmer und trojanische Pferde diskutiert. Im Abschnitt 6 wird die Datenspionage als eine besondere Form der Bedrohung unserer Wirtschaft diskutiert. Schließlich endet der Aufsatz mit der Darstellung von Regulierungsversuchen auf nationaler, europäischer und internationaler Ebene (Abschnitt 7).

2 Bedrohungen

Bedrohungen von IT-Systemen lassen sich grundsätzlich kategorisieren [2] nach Verlust der *Vertraulichkeit*, Verlust der *Integrität* und Verlust der *Verfügbarkeit*.

So können beispielsweise bereits der Ausfall eines Krankenhaus-Informationssystems und die damit verbundene Unverfügbarkeit von Patientendaten (beispielsweise Labordaten) oder die unerkannte Manipulation von Medikationsdaten zu bedrohlichen Situationen führen. Bereits kurzzeitige Ausfälle der Datennetze, die die Handelsplätze und Finanzmärkte miteinander verbinden, können zu hohen finanziellen Verlusten führen.

Das Ausspionieren von Firmengeheimnissen, etwa vertraulichen Forschungsergebnissen, durch die Konkurrenz kann ein Unternehmen in Wettbewerbsnachteile bringen. Selbst unser Telefonnetz, das heute im Innern über ein digitales Netz realisiert ist, und dessen permanente Verfügbarkeit wir mit hoher Selbstverständlichkeit erwarten, ist nicht 100-prozentig vor Bedrohungen geschützt.

Obwohl perfekter und vollständiger Schutz niemals realisierbar ist, sollten präventive Maßnahmen zum Schutz vor diesen Bedrohungen ergriffen werden, um das Risiko zu minimieren.

IT-Sicherheit versucht nun, die Systeme gegen diese Bedrohungen, die sowohl durch Fehlfunktionen und natürliche Phänomene ausgelöst werden können (genannt Fehlertoleranz) als auch gegen „intelligente Angreifer“ zu schützen. Der Schutz vor böswilligen Aktionen setzt ein Modell des unterstellten Angreifers voraus, in dem dessen Stärke beschrieben wird (Angreifermodell). Wissenschaftler versuchen nun, Mechanismen zu finden, die gegen eine definierte Stärke des Angreifers wirken.

Vertraulichkeit

Vertrauliche Daten dürfen nicht in die Hände unberechtigter Personen, Institutionen oder Staaten kommen und sind deshalb vor unberechtigter Kenntnisnahme zu schützen.

Gegen Ausspähen von Daten bei der Übertragung (Verlust von Vertraulichkeit) helfen *Verschlüsselungsverfahren* sowie *Steganographie*. Bei Steganographie werden vertrauliche Informationen in unscheinbare, unverdächtige Hülldaten eingebettet, ohne dass die Existenz der Geheimbotschaft entdeckbar ist.

Zum Schutz vor Informationsflussanalysen (kurz: Verkehrsanalysen) müssen Verfahren zur *Anonymität und Unbeobachtbarkeit* – ebenfalls Vertraulichkeitsaspekte – eingesetzt werden. Anonymität und Unbeobachtbarkeit können durch sog. datenschutzfreundliche Techniken realisiert werden. Solche Verfahren erfordern einen höheren Aufwand als die reine Verschlüsselung der Inhalte. Im Bereich E-Commerce sind die bekanntesten Verfahren, die zur Klasse der anonymen Verfahren zählen, die digitalen anonymen Zahlungssysteme und Verfahren zum unbeobachtbaren Web-Surfen im Internet [3]. In mobilen Kommunikationsnetzen (Mobiltelefon, Mobiles Internet) könnten diese Verfahren auch angewendet werden, um die Aufenthaltsorte mobiler Teilnehmer zu schützen [4], was aus Kostengründen bisher leider unterbleibt.

Integrität

Integere Daten sind unverfälscht und müssen einem Verantwortlichen zurechenbar sein.

Gegen die bewusste Verfälschung von Nachrichten (Verlust an Integrität) können *Message Authentication Codes* eingesetzt werden. Das sind spezielle Prüfsummen, die sofort eine Verfälschung erkennbar machen. Mit Hilfe der *digitalen Signatur* ist Zurechenbarkeit, d.h. die Integrität der Nachricht zusammen mit der Gewissheit über die Authentizität des Absenders, realisierbar: Nachrichten können so ihrem „Unterzeichner“ eindeutig zugeordnet werden.

Verfügbarkeit

Verfügbarkeit bezieht sich sowohl auf Daten als auch auf Kommunikationsdienste, die von jedem, der dazu berechtigt ist, innerhalb vorgegebener Zeitschranken nutzbar sein sollen bzw. ihren Dienst erbringen.

Gegen den Verlust von Verfügbarkeit existieren bisher keine ausgereiften Verfahren. Sog. Denial-of-Service Angriffe führen immer wieder zur Unverfügbarkeit von Internet-Diensten und machen damit die katastrophale Situation deutlich. Besonders für E-Commerce-Firmen, für die die Verfügbarkeit des Internet die geschäftliche Basis ist, kann dies zu hohen finanziellen Verlusten und Imageschäden führen, wenn deren Dienste angegriffen werden. Solche Formen der Störung werden neuerdings auch als Cybercrime bezeichnet. Die Verfügbarkeit von Daten und Diensten kann erreicht werden durch Diversität und redundante Auslegung von Leitungskapazitäten, Rechenressourcen und Datenspeichern.

Eine ausführliche Darstellung der Basistechnologien zum Schutz vor intelligenten Angreifern ist z.B. in [5, 6] zu finden. In den folgenden Abschnitten werden vier typische und weit verbreitete Bedrohungen erläutert: Denial-of-Service Angriffe, fehlerhafte Software, die Virenproblematik und Datenspionage.

3 Denial-of-Service Angriffe

Während in klassischen Telekommunikationsnetzen (Telefonnetze) aufgrund begrenzter Ressourcen eine Mangelverwaltung (und damit Ressourcenökonomie) von Bandbreite und anderen Betriebsmitteln auf sehr niedriger technischer Ebene vorgenommen wurde und wird, arbeitet das Internet weitgehend ohne derartige Zuweisungen und ist somit anfällig für Denial-of-Service-Angriffe durch sog. Flooding.

Die Entwicklung des Internet hat seine Ursprünge im militärischen Bereich. Man wollte ein dezentralisiertes Kommunikationsnetz, bei dem der Ausfall einzelner Rechner oder Kommunikationsverbindungen – etwa nach einem atomaren Angriff des Gegners – nicht zum Totalausfall des gesamten Netzes führte. Die hohe Verfügbarkeit erreicht man durch mehrfach redundante Vernetzung der Rechner und alternative Routen zum Transport der Daten. Somit ist es tatsächlich fast ausgeschlossen, den Datentransport im Internet vollständig zu stören. Punktuelle Angriffe führen nur zu punktuellen Ausfällen der Kommunikation. Voraussetzung ist allerdings, dass die konzeptionell vorgesehene Verteiltheit und mehrfach redundante Wegewahl tatsächlich realisiert wird. Dies ist im heutigen Internet nicht unbedingt der Fall. So sind beispielsweise die deutschen Internet Service Provider über einen zentralen Austauschpunkt (DE-CIX, Deutscher Commercial Internet Exchange) untereinander verbunden [7]. Der DE-CIX stellt außerdem die Hauptverbindungen von Deutschland nach Großbritannien und USA her. Ein Ausfall des DE-CIX würde somit zur weitgehenden Unverfügbarkeit der innerdeutschen und transatlantischen Internetkommunikation führen [8].

Das Internet besteht nun nicht nur aus einem theoretisch hochverfügbaren Transportsystem, sondern auch aus einzelnen Internet-Diensten (E-Mail, World Wide Web, News etc.). Die Internet-Dienste erreichen jedoch bei weitem nicht die hohe Verfügbarkeit des zugrunde liegenden Transportsystems. Sie sind vielmehr stark anfällig gegen gezielt herbeigeführte Ausfälle durch intelligente Angreifer (Denial-of-Service oder kurz DoS).

Ein sehr einfacher Denial-of-Service Angriff ist das E-Mail-Bombing. Hier werden durch einen Angreifer sehr viele und sehr große E-Mail-Nachrichten an einen einzelnen Empfänger oder eine Gruppe versendet. Die Nachrichten enthalten meist unsinnige, aber sehr große Dateianhänge (Attachments), deren Zweck es ist, den vorhandenen Speicher auf dem Mail-Server des Empfängers auszuschöpfen, bis die tatsächlichen Nachrichten mangels Speicher abgewiesen werden müssen. Spamming gleicht somit dem Verstopfen des Postbriefkastens. Da ein Mail-Server meist mehrere Benutzer (z.B. alle Mitarbeiter eines Unternehmens) verwaltet, sind durch einen solchen Angriff gleich mehrere Benutzer oder sogar das ganze Unternehmen betroffen.

Weiterhin könnte ein Angreifer versuchen, die Website eines Unternehmens derart häufig abzurufen, dass der Rechner (Webserver) überlastet wird und die regulären Anfragen nicht mehr bedienen kann und unter der Last zusammenbricht. Hierzu sind – wie beim Mail-Bombing – seitens des Angreifers keinerlei Hackermethoden, d.h. Einbrüche in fremde Rechner, erforderlich. Er muss nur die nötige Menge Verkehr produzieren. Da der angegriffene Server förmlich mit Nachrichten überflutet wird, sind diese Angriffe auch Beispiele für Flooding-Angriffe.

Der Webserver könnte nun „aufrüsten“ und seinen Server mehrfach redundant ausführen, so dass ein einzelner Angreifer niemals die nötige Last erzeugen kann, um alle Server zu blockieren. Unternehmen, die auf die Verfügbarkeit ihrer Internet-Dienste angewiesen sind (z.B. Web-Portale, Internet-News-Services, Online-Shops) gehen tatsächlich diesen Weg. Die Angreifer haben jedoch ebenfalls aufgerüstet: Mittels sog. distributed Denial-of-Service (dDoS) Angriffe gelang es ihnen beispielswei-

se, die Webserver der Firmen Yahoo.com und Amazon.com für mehrere Stunden unverfügbar zu machen [9]. Bei dDoS-Angriffen bemächtigt sich der Angreifer (meist mittels Hacker-Methoden) vieler schlecht gesicherter fremder Rechner, die er zur Erzeugung des nötigen Datenverkehrs missbraucht. Er flutet gewissermaßen das Opfer von mehreren Stellen gleichzeitig.

4 Fehlerhafte Software

Neben Flooding beruhen viele erfolgreiche Denial-of-Service Angriffe auf fehlerhafter Software. So könnte ein Angreifer beispielsweise durch Ausnutzung eines Programmierfehlers den Server zum Absturz zu bringen. Ein kleines Programm, das solche Angriffe ohne weiteres Wissens – sozusagen mit einem Doppelklick – realisierbar macht, wird als Exploit bezeichnet. Exploits werden von Hackern veröffentlicht, um den Fehler bzw. die Schwachstelle sichtbar zu machen und die Anwender dadurch für die Sicherheitsproblematik zu sensibilisieren. Beispiele für bekannte Exploits für die Windows-Betriebssysteme sind WinNuke und TearDrop [10]. Sie führen zum Stillstand des Rechners und erfordern schließlich ein Reboot. So wurden beispielsweise im sehr weit verbreiteten Programm BIND, das in Firmennetzen und bei Internet Service Providern die Umsetzung von IP-Nummern zu den Rechnernamen im Domain Name Service (DNS) vornimmt, entsprechende Lücken entdeckt [11].

Man kann davon ausgehen, dass die Zahl tatsächlich existierender Exploits deutlich höher liegt als die Zahl bekannter Exploits. Nicht alle Hacker veröffentlichen ihr Wissen, weil sie sich sonst Aufträge im Bereich der Wirtschafts- und Industriespionage nicht mehr so gut erfüllen ließen: Noch schlimmer als DoS-Exploits sind solche, die einem Hacker Administratorrechte auf dem angegriffenen Rechner verleihen. Ein Angreifer kann dann nicht nur die Verfügbarkeit beeinträchtigen, sondern gleichfalls die Vertraulichkeit und Integrität von Daten und Diensten.

Auf diese Weise berühmt geworden ist beispielsweise die Software WU-FTP, die einen FTP-Server (FTP: File Transfer Protocol) realisiert. WU-FTP ist unter den Linux-Betriebssystemen weit verbreitet. Für WU-FTP wurden wiederholt Exploits veröffentlicht, die – durch einen sog. Buffer Overflow ausgelöst – einem Hacker Administratorrechte auf dem Server verliehen. Das Sicherheitsloch wurde zwar durch Security-Updates jeweils gestopft, allerdings informieren sich Benutzer vielfach nicht über neue Versionen und Sicherheitslücken der auf ihrem Rechner installierten Software und setzen sich so unwissentlich einem hohen Risiko aus.

Manche Angriffsprogramme zur Ausführung von Exploits oder DoS-Angriffen sind überraschend komfortabel bedienbar. Die Benutzungsschnittstellen sind teilweise sehr übersichtlich und selbsterklärend. Sie sind „kinderleicht“ zu bedienen, im Internet frei verfügbar und sogar auf CD [12] im Buchhandel veröffentlicht, natürlich stets mit dem Hinweis, dass sie nicht zum Angreifen fremder Rechner benutzt werden dürfen, sondern als Analysewerkzeuge zum Testen der eigenen Sicherheit vor Angriffen dienen. Somit existieren kaum noch technische Hürden, die die normale PC-Benutzer überwinden müssen, um zu Hackern zu werden. Dadurch unterschätzen die naiven Hobby-Hacker – manchmal auch Script-Kiddies genannt – schnell die Ernsthaftigkeit und Strafbarkeit solcher Angriffe.

5 Computerviren, Würmer und trojanische Pferde

Eine der sehr ernst zu nehmenden Bedrohungen der Zukunft für unsere Gesellschaft sind Computerviren, Würmer und trojanische Pferde. Sie haben gemeinsam, dass sie eine ungewollte Schadensfunktion ausführen, die sich auf alle drei Bedrohungen (Vertraulichkeit, Integrität, Verfügbarkeit) erstrecken kann. Computerviren besitzen darüber hinaus einen Mechanismus zur Replikation, der es ihnen ermöglicht, sich auf lokale Dateien auszubreiten. Würmer können sich sogar über Computernetze ausbreiten, z.B. indem sie sich selbst an die E-Mail-Adressen eines lokalen Adressbuches versenden.

Computerviren und Würmer verursachen schon heute gravierende finanzielle Schäden in Unternehmen. Durch ihre unkontrollierbare Verbreitung über das Internet „verstopfen“ sie Mail-Accounts und damit fremde Server (Verlust der Verfügbarkeit), zerstören und manipulieren (Verlust der Integrität) möglicherweise Daten und können sogar Geschäftsgeheimnisse ausspionieren und unbefugt nach außen transportieren (Verlust der Vertraulichkeit).

Ein Beispiel für einen besonders aggressiven und mit hohen Schäden verbundenen Virus ist der Loveletter-Virus (auch I-love-you-Virus), der sich über das Adressbuch der E-Mail-Software Microsoft Outlook verbreitete und neben verstopften digitalen Postfächern auch Dateien auf lokalen Festplatten zerstörte und veränderte. Der Virus besteht aus etwa 300 Zeilen Quellcode der Sprache Visual Basic.

Backorifice ist ein trojanisches Pferd für Windows-Betriebssysteme, das einem Angreifer unbemerkt die vollständige Kontrolle über sein Opfer gibt, da der angegriffene Rechner vollständig ferngesteuert werden kann. Backorifice wird deshalb auch gern als „Fernwartungswerkzeug“ eingesetzt.

Die meisten der moderneren Viren und Würmer wurden von ihren Entwicklern ohne ein spezifisches Infektionsziel (Opfer) entwickelt. Vielmehr ging es um die schnelle und zahllose Verbreitung und den schnellen, aber kurzzeitigen und zweifelhaften Ruhm seines Programmierers. Durch die Monokultur bei den verwendeten Betriebssystemen und der Anwendungssoftware können vorhandene Schwächen der (System)-Software vielfachen Schaden anrichten. Nicht vorhandene oder ungeeignete Zugriffskontrollmechanismen (beispielsweise Schreibrechte auf ausführbaren Dateien, automatisches Öffnen bzw. Ausführen von E-Mail-Attachments) verschlimmern die Situation.

Inzwischen ist festzustellen, dass die Angriffswerkzeuge immer universeller werden und gleichzeitig konvergieren. Der Internet-Wurm Code Red, der hauptsächlich im Juli 2001 auftrat, nutzte beispielsweise gleichzeitig einen Programmierfehler in Microsofts Webserver ISS aus, enthielt gewissermaßen auch ein Exploit. Code Red replizierte sich zunächst auf viele ISS-Server. Die befallenen Rechner wurden schließlich für eine dDoS-Attacke auf den Webserver des Weißen Hauses missbraucht. Im August 2001 tauchte ein neuer Wurm namens Code Red II auf, der auf den befallenen Servern eine Hintertür installierte, mit dem das Opfer ferngesteuert werden konnte, beispielsweise um das Ziel einer dDoS-Attacke festzulegen.

Der Internet-Wurm Nimda (rückwärts geschrieben gelesen: Admin), der erstmals am 18. September 2001 entdeckt wurde, benutzt ebenfalls mehrere Methoden, um sich fortzupflanzen und Schaden anzurichten. Zunächst sucht Nimda nach Microsoft ISS-Servern, versucht dann in diese einzudringen und kopiert sich bei Erfolg unter dem Namen Admin.dll dorthin. Anschließend verschickt er sich selbst an alle E-Mail-Adressen eines etwa vorhandenen Adressbuches. Der Empfänger erhält den Wurm als Anlage mit dem Namen readme.exe, die von Microsoft Outlook und Outlook Express automatisch geöffnet (hier: gestartet) wird. Handelt es sich bei dem infizierten Op-

fer um einen Webserver, werden alle webbezogenen Dateien um ein Stückchen Code erweitert. Besucht ein Surfer eine der maipulierten Webseiten, wird unbemerkt ein ausführbare Datei readme.eml heruntergeladen, die ebenfalls den Virus enthält. Sofern JavaScript im Web-Browser aktiviert ist, wird readme.eml bei einigen Browsern (z.B. Internet-Explorer) automatisch gestartet, in alle schreibbaren Netzwerkverzeichnisse kopiert und der Replikationsmechanismus beginnt von vorn. Wenn sich mehrere Benutzer Verzeichnisse teilen, werden deren Dateien beim Zugriff auf das Verzeichnis ebenfalls infiziert. Zusätzlich installiert Nimda auf dem infizierten Rechner noch eine Hintertür, indem der den Benutzer *Guest*, der unter Windows kein Passwort benötigt, zum Mitglied der *Administrators*-Gruppe macht.

Viren und insbesondere trojanische Pferde eignen sich auch für die gezielte Schädigung eines Opfers. Sie könnten – lange bevor sie ihren Schaden anrichten sollen – unbemerkt platziert werden und so programmiert sein, dass sie ihren Schaden erst nach einer Handlungsanweisung durch den Angreifer auslösen. So könnten Unternehmen, Finanzmärkte und Behörden bereits lange „verseucht“ sein, ohne dass dies den Verantwortlichen bekannt wäre. Das Heimtückische an dieser Bedrohung ist, dass die Überprüfung der Computersysteme auf das Vorhandensein von trojanischen Pferden und der zweifelsfreie Ausschluss dieser Bedrohung nicht möglich sind, da man einem trojanischen Pferd die „Hinterlist“ eben nicht ansieht. Virenscanner und Firewalls stellen somit keinerlei Schutz vor dieser speziellen Bedrohung dar.

6 Datenspionage

Je mehr Daten über Kommunikationsnetze ausgetauscht werden, umso wahrscheinlicher wird es für einen Angreifer, darunter auch sensible Informationen – z.B. Geschäftsgeheimnisse oder Privates – zu finden. Solange Daten nicht verschlüsselt übermittelt werden, können Sie sehr leicht mitgelesen werden. Zwar sind Verschlüsselungstechnologien inzwischen ausgereift und entsprechende Produkte verfügbar, jedoch werden sie aus Bequemlichkeit, Unwissen oder Dummheit noch nicht überall dort angewendet, wo auch sensible Daten anfallen.

Beispiele für die breite Verfügbarkeit und hervorragende Bedienbarkeit von Verschlüsselungssoftware sind die Programme Pretty Good Privacy (PGP) [13] und Gnu Privacy Guard (GnuPG) [14], mit denen heute private wie auch geschäftliche E-Mails und Dateien sicher verschlüsselt werden können.

Dass Kommunikationsverbindungen tatsächlich belauscht und überwacht werden, bezweifelt heute niemand mehr. Das Überwachungssystem Echelon [15] soll beispielsweise dem amerikanischen Geheimdienst Informationen aus der Überwachung von internationalen Telefonverbindungen, E-Mails und Satellitenkommunikation liefern. Man kann davon ausgehen, dass nicht nur westliche Geheimdienste mit solchen Methoden schnüffeln, wenn auch vielleicht mit weniger Ressourcen und weniger Hightech.

Verschlüsselung hilft gegen Mitlesen der Inhalte auf den Kommunikationsstrecken und erlebt derzeit seine weite Verbreitung. Beim Empfänger müssen die Nachrichten jedoch entschlüsselt werden und liegen somit auch dort im Klartext vor. Deshalb versuchen die Angreifer neuerdings verstärkt, direkt beim Rechner des Senders oder Empfängers anzugreifen, z.B. mittels trojanischer Pferde oder Hackermethoden. Auch Strafverfolger benutzten bereits solche Mittel. So soll das amerikanische FBI die Tastatureingaben eines Verdächtigen angezapft haben, um an verschlüsselte Dateien zu kommen [16].

Durch Ausnutzung von Konfigurations- und Programmierfehlern (meist Buffer

Overflows) in Serveranwendungen (z.B. File Transfer zum Datenaustausch zwischen den Filialen einer Bank) kann ebenfalls Datenspionage betrieben werden. Hierzu wird in den Rechner des Opfers – ausgelöst durch einen Ausnahmezustand der Serversoftware, die vom Programmierer so nicht beabsichtigt war – eingebrochen. Der Angreifer kann dann beliebige Aktionen auf dem Server ausführen: Er kann Daten kopieren, verändern oder löschen.

Einem Betrüger gelang es beispielsweise mit Hilfe von ausgespähten Sozialversicherungsnummern, im Namen seiner Opfer Kreditschecks über Beträge von bis 44.000 Dollar zu erhalten und damit einkaufen zu gehen [17].

7 Regulierungsversuche

Um der bedrohten Sicherheit der Informationsnetze zu begegnen, hatte die Bundesregierung im April 2000 die Task-Force „Sicheres Internet“ [18, 19] eingerichtet und einen Katalog mit 15 Sofortmaßnahmen zur Eindämmung der Internetkriminalität vorgelegt. Angesichts der Internationalität des „Netzes der Netze“ ist der Nutzen nationaler Regelungen allerdings recht begrenzt, da Kriminelle in Zonen, Regionen und auf Server ausweichen können, für die die nationalen Regelungen nicht gelten.

Der Europarat hat auf die neuen Risiken beispielsweise mit der „Cybercrime Convention“ [20] reagiert, die der Anfang eines internationalen Regelungswerkes zur Verfolgung von Straftaten – insbesondere DoS-Angriffen, Verletzungen des Urheberrechts und Bereitstellung anderer illegaler Inhalte – im und durch das Internet sein soll. Dann wären auch Besitz und Herstellung von Anleitungen und Software zur Begehung von Computerkriminalität strafbar.

Ein weiterer Versuch zur Harmonisierung der Gesetze, die das Internet besser regulierbar machen sollen, ist die „Hague Convention on Jurisdiction and Foreign Judgments in Civil Matters“ [21].

Juristische Regeln allein werden Angriffe nicht verhindern können: Gesetzlose lassen sich leider nicht durch angedrohte Strafen abschrecken. Deshalb muss der Schutz der Informationsnetze auch auf technischer Ebene und präventiv erfolgen. Da hundertprozentige Sicherheit in der Praxis niemals erreichbar ist, kommt es wenigstens darauf an, Bedrohungen rechtzeitig zu erkennen und Schutzmaßnahmen zu treffen, damit die Risiken beherrschbar sind und möglichst minimiert werden können.

Literatur

[1] Berliner Zeitung, 15. Nov. 2001. Seite 3.

[2] Viktor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols. ACM Computing Surveys 15/2 (1983) 135–170.

[3] The JAP Anonymity & Privacy Homepage. http://anon.inf.tu-dresden.de/.

[4] Hannes Federrath: Sicherheit mobiler Kommunikation. DuD Fachbeiträge. Vieweg, Wiesbaden, 1999. Info: http://www.inf.tu-dresden.de/~hf2/mobil/buch.shtml.

[5] Hannes Federrath, Andreas Pfitzmann: Datenschutz und Datensicherheit. In: Uwe Schneider, Dieter Werner (Hg.): Taschenbuch der Informatik. Fachbuchverlag Leipzig im Carl Hanser Verlag, München, 3. Aufl., 2000, 586–604.

[6] Hannes Federrath, Andreas Pfitzmann: Bausteine zur Realisierung mehrseitiger Sicherheit. In: Günter Müller, Andreas Pfitzmann (Hg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison-Wesley-Longman, 1997, 83–104. http://www.inf.tu-dresden.de/~hf2/publ/1997/FePf_97Baust/.

[7] The DE-CIX (Deutscher Commercial Internet Exchange). http://www.de-cix.net/.

[8] Cyberterror: Internet-Infrastruktur gefährdet? Elektronischer Terrorismus und die Folgen. ct 25 (2001).

[9] Florian Rötzer: Sicherheitshysterie. Telepolis, 13. Febr. 2000. http://www.heise.de/bin/tp/issue/dl-artikel.cgi?artikelnr=5785&mode=html.

[10] Nuke Information and Patches. http://www.irchelp.org/irchelp/nuke/info.html.

[11] Silicon-News: Großes Sicherheitsrisiko bei Domain-Servern. http://www.silicon.de/a40853.

[12] Datenschutz-CD 2001. Hacker's Best friend. CD-ROM für Windows ab 95, NT/2000 und Linux. Utech-Verlag, Oldenburg, 2001.

[13] The International PGP Homepage. http://www.pgpi.org/.

[14] The Gnu Privacy Guard Homepage. http://www.gnupg.org/.

[15] Interception capabilities 2000. http://www.iptvreports.mcmail.com/ic2kreport.htm.

[16] Florian Rötzer: Nichts mehr mit Pretty Good Privacy? Telepolis, 6. Dez. 2000. http://www.heise.de/tp/deutsch/inhalt/te/4418/1.html.

[17] Heise-News: Identitätsklau via Internet, 4. Sept. 2000. http://www.heise.de/newsticker/data/jk-04.09.00-000/.

[18] Heise-News: Schily empfiehlt Sofortmaßnahmen für sichereres Internet, 25. Apr. 2000. http://www.heise.de/newsticker/data/fm-25.04.00-000/.

[19] Frank W. Felzmann: Die Task Force „Sicheres Internet". KES Zeitschrift für Kommunikations- und EDV-Sicherheit 16/3 (2000) 61–68.

[20] Draft Convention on Cybercrime. http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm.

[21] Julia Lawlor: From the Trenches: Do laws know no bounds?, 16. Okt. 2001. http://www.redherring.com/index.asp?layout=story_imu&doc_id=1570020357&channel=10000001.

Über den Autor

Hannes Federrath, Dr.-Ing., studierte von 1989 bis 1994 Informatik und promovierte 1998 an der Technischen Universität Dresden auf dem Gebiet der Sicherheit mobiler Kommunikation. Von 1994 bis 1999 war er als wissenschaftlicher Mitarbeiter, seit 1999 ist er als Oberingenieur im Bereich Informations- und Kodierungstheorie bei

Prof. Andreas Pfitzmann tätig. Von September 1999 bis August 2000 forschte er als Gastwissenschaftler am International Computer Science Institute Berkeley, Kalifornien. Von September 2000 bis August 2001 forschte und lehrte er am Institut für Informatik der Freien Universität Berlin. Forschungsschwerpunkte sind Sicherheit in verteilten Systemen, Kryptographie, Steganographie, Anonymität und Unbeobachtbarkeit sowie Mobile Computing.