OM 7/8 Titelgeschichte
Ergebnis des Interviews mit dem CCC von Chr. D vom Mai 1989

Beratung durch Hacker

Datenschutz und Datensicherung aus Sicht des Chaos Computerclubs e.V.

Die Aktivitäten des Chaos Computerclubs, kurz CCC, sind nicht unumstritten. Nur wenigen ist bekannt, daß sich die Mitglieder dieses Vereins auch intensiv mit dem Problem der Datensicherheit auseinandersetzen.
Mit den CCC Mitgliedern Erich Margrander, Bernd Fix und Wau Holland sprach für die OM-Redaktion Christine Dählmann.

Chaos Computerclub - dieser Name wird vielfach mit 'den Hackern' schlechthin gleichgesetzt. Zwar läßt sich dieses Image nicht so schnell ausräumen, aber von Fachkreisen werden die Mitglieder des CCC immer stärker als Computerfachleute anerkannt - als ernsthafte Berater, die sich nicht nur in technischen Dingen auskennen, sondern sich auch Gedanken über unsere wirtschaftliche und gesellschaftliche Zukunft machen.

Absolute Sicherheit

In Datenschutz und Datensicherung, also die Datensicherheit insgesamt, wird in vielen Unternehmen immer mehr Zeit und Geld investiert. Auf diese Weise, so glaubt man, kann man alle Versuche, von Außen unbefugt in das Computersystem eines Unternehmens einzudringen, verhindern.

Nach Auffassung der Mitglieder des CCC leider ein vergebliches und ausgesprochen uneffizientes Unterfangen. Ihrer Meinung nach ist es prinzipiell unmöglich, ein Computersystem, das mit der Umwelt Daten austauscht und nicht isoliert eingesetzt wird, absolut sicher gegen Eindringlinge zu machen. Im Gegenteil, jede Verbesserung der Hard- oder Software fordert nur die Kreativität der meist jugendlichen Hacker aufs neue heraus, anstatt sie abzuschrecken.
Eine Anleitung, wie man den kleinen Fehler im Betriebssystem, die winzige Lücke durch die man in einen Computer eindringen kann findet, gibt es im Prinzip nicht. Das 'Hacken' ist meist eine sehr zeitintensive Beschäftigung, die sich über Monate hinziehen kann. Um ans Ziel zu gelangen, bedarf es nicht nur einer ungeheuren Ausdauer und viel Glück, sondern auch eines immensen Fachwissens, das sich die Meisten durch Erfahrung selbst angeeignet haben.

Nach Ansicht des CCC ist es notwendig erst einmal grundsätzlich zu akzeptieren, daß es keine vollkommene, technische Computersicherheit gibt. Da Computertechnik nicht absolut beherrschbar, nicht völlig sicher zu machen ist, muß man versuchen sie auf sozialem Wege zu kontrollieren. Das heißt, daß man sich bereits vor jedem Computereinsatz über die möglicherweise damit verbunden Gefahren im Klaren sein sollte. Ist es beispielweise zu verantworten, einem Computer die Steuerung eines Atomkraftwerkes zu überlassen ?
Die Computertechnologie an sich ist durchaus nicht negativ. Erst die Einsatzform entscheidet darüber, ob sie der Entwicklung von Wirtschaft und Gesellschaft förderlich ist.

Praktikable Datensicherheit

Die Mitglieder des CCC sind zwar davon überzeugt, daß es unmöglich ist ein Computersystem technisch vollkommen abzuschotten, aber sie sehen durchaus Möglichkeiten die Daten selbst sicher zu machen. Das beginnt bereits bei ihrer Organisation: Sensible Daten, also diejenigen Informationen, die auf keinen Fall in fremde Hände gelangen sollen, dürfen

entweder gar nicht erst auf einem Rechner gespeichert werden, oder, etwas praktischer, sie werden grundsätzlich nur in verschlüsselter Form abgelegt. Selbst wenn sich jemand unbefugt Zugang zum Computer verschaffen kann, wird es ihm kaum möglich sein den Inhalt des vorgefundenen Datengewirrs zu verstehen.

Das Verschlüsseln selbst ist im Prinzip eine einfache Angelegenheit, für die es bereits fertige Programme gibt, wie beispielsweise 'PC - DES' von Bernd Fix (CCC). Dieses DES - Verfahren ist so sicher, daß es bisher nicht einmal der NSA (National Security Agency als amerikanischer Nachrichten- und Geheimdienst) gelungen ist, an den Inhalt von mit DES verschlüsselten Dateien zu gelangen. Aufgrund der immensen Anzahl von Möglichkeiten, die man durchprobieren müßte wäre es einfacher, die Person, die das Codewort kennt, zu dessen Herausgabe zu veranlassen, oder nach einem Versteck des Schlüssels zu suchen.

Der Schlüssel - darin liegt der große Schwachpunkt: Das Verfahren kann noch gut sein, wenn der dazugehörige Schlüssel nur unzureichend verwahrt ist, oder so gewählt wird, daß sich die Anzahl der Lösungsmöglichkeiten wesentlich verringert (zum Beispiel wenn bekannt ist, daß nur ein Monatsname als Codewort in Frage kommt), wird jedes Verschlüsseln nutzlos. In ruhigem Vertrauen auf die Sicherheit des Verschlüsselns, sind solche organisatorischen Mängel nach Meinung des Chaos Computerclubs leider weiter verbreitet, als man glauben würde. Die Technik kann aber, wie so oft, nur Unterstützungsfunktion haben. Sie nimmt es dem Menschen nicht ab die wirkliche Sicherheit in seinem Kopf zu produzieren - durch Auswahl und Aufbewahrung des Schlüssels.

Computerviren

Es scheint inzwischen fast zu einer Art Mode geworden zu sein: Früher war einfach der Computer schuld wenn was nicht ging - heute ist es ein Virus.
Aber die Gefahr von Computerviren ist nicht zu unterschätzen. Nach Meinung der CCC Mitglieder stammen die Viren, die in das Computersystem eines Unternehmens eingeschleust werden, zu weit über 90 Prozent von internen Mitarbeitern und kommen nur in den seltensten Fällen von Außen. Für einen Insider ist es auch wesentlich einfacher einen Virus einzubringen. Oft sind es Mitarbeiter, die mit ihrem Job unzufrieden sind, oder einfach Angst vor einer Entlassung haben. Als eine Art Kündigungsschutz wird dann kurzerhand ein Virus eingebaut. Solange das Arbeitsklima unbefriedigend ist und sich Mitarbeiter in zu großer Abhängigkeit fühlen, solange wird es auch Computerviren geben. Viren sind nach Ansicht des CCC nie Selbstzweck, sondern immer Ausdruck einer inneren Stimmung.

Computerkommunikation

Weitaus größere Probleme bringt der Datenaustausch im Netz mit sich: Wie kann man sicher sein, daß die empfangene Sendung tatsächlich vom angegebenen Absender stammt und daß die Daten nicht während der Übermittlung in irgend einer Form manipuliert wurden?
Genau diese Frage wird durch die sogenannte 'elektronische Unterschrift' beantwortet. Sie stellt sicher, daß Inhalt und Absender der Nachricht authentisch sind, sie kann aber nicht dafür garantieren, daß keine Nachricht abgefangen wurde.
Das asymmetrische Verschlüsselungsverfahren RSA (Rivest, Shamir, Adleman) auf dem die elektronische Unterschrift beruht, gilt zwar als mit den heutigen technischen Möglichkeiten nicht zu 'knacken', hat aber den großen Nachteil, daß es bei einem Netz mit mehr als hundert Benutzern eine zentrale Schlüsselvergabestelle geben muß.
Darin sehen die Mitglieder des Chaos Computerclubs in zweierlei Hinsicht ein Problem:

Zum einen arbeitet auch diese Zentrale mit Computern. Deren Manipulation könnte unabsehbare Folgen für die Verläßlichkeit des elektronischen Dokumentenaustausches haben.
Wesentlich problematischer stellt sich aber die ungeheure Machtposition, dieser zentralen Schlüsselvergabestelle dar. Sie resultiert aus der Tatsache, daß die Vergabestelle nicht nur den allgemein zugänglichen, sogenannten 'öffentlichen Schlüssel' generiert, sondern auch den, aufgrund des komplizierten Algorithmus davon abhängigen, 'persönlichen Schlüssel' vergeben muß, um das komplizierte Gesamtsystem zu koordinieren. Die Zentrale ist somit über die geheimen Schlüssel aller Benutzer des Netzes informiert und könnte sich - wenn sie wollte - jederzeit Zugang zu persönlichen Daten verschaffen. Wer die Schlüsselvergabestelle beherrscht hat die Macht den gesamten Nachrichtenaustausch im Netz zu überwachen und zu manipulieren.

Der Vorteil eines solchen Public-key Verfahrens liegt darin, daß man, im Gegensatz zu anderen Verschlüsselungsverfahren wie beispielsweise DES, nicht vor dem Problem steht mit jedem Datenempfänger persönlich und auf möglichst sicheren Wegen einen geheimen Schlüssel vereinbaren zu müssen. Öffentliche Systeme sind organisatorisch also wesentlich praktischer zu handhaben und werden deshalb zunehmend entwickelt und forciert.

ISDN

Voraussichtlich wird die Verschlüsselung von Daten in Zukunft noch an Bedeutung gewinnen, denn leider ist auch das ISDN - Netz nicht vollkommen abhörsicher. Auch Glasfaser kann nach Aussage des Computerclubs angezaft werden, wenngleich man dort natürlich wesentlich größere Datenmengen auseinander zu filtern hat.

Die eigentliche Kritik der Mitglieder des CCC setzt aber bereits bei der Organisation des Netzes an.
Durch die Einführung von ISDN wird es möglich und teilweise auch notwendig, wesentlich mehr Aktivitäten der Nutzer zu speichern. Mit diesen Daten wäre es relativ einfach umfassende Bewegungsbilder einzelner Personen zu erstellen (zum Beispiel wie oft und wann, wer mit wem, wie lange telefoniert hat). Es ist äußerst fraglich, ob die Speicherung bestimmter persönlicher Daten durch ISDN überhaupt mit dem vom Bundesgerichtshof garantierten Recht auf informationelle Selbstbestimmung in Einklang zu bringen ist.

Selbst wenn man davon ausgeht, daß, wie von einigen Politikern immer wieder betont wird, eine derartige Überwachung zwar prinzipiell möglich ist, aber in unserem demokratischen Staat nicht genutzt wird, ist das keine endgültige Garantie. ISDN ist immerhin eine Technologie, die langfristig auf die Zukunft hin ausgerichtet ist. Die Vergangenheit hat uns gelehrt, daß in einem solchen Zeitraum die Staatsform der Bundesrepublik Deutschland einige Male wechseln kann. Wer von den heutigen Politikern kann daher garantieren, daß auch in Zukunft keine Regierung mit ganz anderen Absichten das Netz kontrolliert. Eine theoretisch perfekte Überwachungstechnik ist dann bereits installiert, während alle bisherigen Kommunikationswege weitgehend aufgehoben wurden.

Damit ist bereits ein weiterer Kritikpunkt des Chaos Computerclubs angedeutet: ISDN ist in der Endstufe als allumfassendes, integriertes Netz geplant, daß nach Auskunft der Post über elf Haupvermittlungsrechner gesteuert wird. Es ist vorgesehen, neue Software immer nur in einen Computer einzugeben und an die anderen zehn Rechner zu überspielen. Das bedeutet, daß es für einen Totalausfall des gesamten ISDN - Netzes theoretisch ausreichen würde, wenn ein unlauterer Mitarbeiter im Rechenzentrum einen entsprechenden Virus in den Hauptcomputer einschleust. Da es im Zeitalter des ISDN keine Ausweichmöglichkeiten mehr geben wird, hieße das letztlich, daß in der ganzen Bundesrepublik Deutschland keine Kommunikation mehr möglich wäre - bis auf Amateurfunk.

Zugegebenermaßen ist das eine - heute noch - utopische Vorstellung, aber, wie die Post dem CCC bestätigen mußte, theoretisch durchaus möglich. Die Folgen eines derartigen Zusammenbruchs für Wirtschaft und Gesellschaft sind nicht einmal annähernd abzuschätzen.

Sicherheit durch Öffnung

Nach Ansicht des CCC wird viel zu viel Geld, Zeit und menschliche Energie darauf verwendet, Hacker zu bekämpfen und zu versuchen Computersysteme abzuschotten. Diese Ressourcen könnten wesentlich kreativer genutzt werden.
Das würde voraussetzen, daß Unternehmer, aber auch Politiker akzeptieren, daß größere Computersicherheit nicht durch immer strengere Gesetze und eine stärkere Abgrenzung zu erreichen ist, sondern im Gegenteil, nur durch die Freigabe von Information. Hinter dieser, für viele wohl etwas ungewöhnlich und unrealistisch erscheinenden Forderung, steht die Vorstellung, daß die Gefahr, daß in Unternehmensdaten eingebrochen wird, in gleichem Maße abnimmt, in dem Datenbanken öffentlich zugänglich gemacht werden und Information frei zur Verfügung gestellt wird. Diese Auffassung läßt sich mit der Erfahrung der letzten Jahre begründen, die gezeigt hat, daß meist aus reiner Neugierde in Computersysteme eingebrochen wird. Dabei stellt es natürlich einen umso größeren Anreiz dar, wenn das jeweilige Unternehmen als vollkommen sicher gilt. Da diese Jugendlichen oft noch nicht zu echter Verantwortung fähig sind, besteht die Gefahr von Kurzschlüssen, wenn sie zufällig auf brisante Informationen stoßen, die sie überfordern.

Abgesehen davon, daß die Freigabe von Information somit den Unternehmen selbst dienlich sein kann, handelt es sich dabei auch um eine Forderung, die nach Ansicht des CCC im gesamtgesellschaftlichen Interesse liegt: Umso mehr Wissen verfügbar ist, desto stärker wird die Entwicklung der ganzen Gesellschaft gefördert. Die durch die informationstechnologische Entwicklung in Gang gesetzten, gesellschaftlichen Veränderungen, werden in Zukunft immer stärker die Freigabe

von Information fordern. Nur wenn der gesellschaftliche Wandel rechtzeitig beachtet wird, gibt es fließende Übergänge und keine teuren Brüche.
Um Mißverständnisse zu vermeiden bleibt noch hinzuzufügen, daß sich diese Forderung selbstverständlich nicht auf sensible Daten, wie beispielsweise die Personaldatendatei oder neueste Forschungsergebnisse bezieht. Gerade solche Daten sollten, wie bereits beschrieben, besonders geschützt und nur in verschlüsselter Form verwahrt werden. Es geht hier um allgemeines Wissen. Dessen Freigabe würde nach Ansicht des CCC ein hohes Maß an Befriedung in die Gesellschaft bringen. Die Möglichkeit frei an wirklich interessierende Informationen zu gelangen, die nicht vorgesiebt oder manipuliert sind, entspricht dem Ideal des CCC - die informierte Gesellschaft (im Gegensatz zur reinen Informationsgesellschaft).

Ziele

Es ist nicht das Hauptanliegen des Chaos Computerclubs der deutschen Wirtschaft zu helfen, aber da sich die Mitglieder des CCC gesamtgesellschaftlicher Zusammenhänge durchaus bewußt sind, ist ihnen klar, daß in dem Moment, in dem die Wirtschaft lahmgelegt wird (zum Beispiel durch den Ausfall des ISDN Netzes) auch jeder einzelne Bundesbürger davon betroffen ist. Daher ist es dem CCC ein Anliegen gerade in der Wirtschaft Veränderungen zu katalysieren, neues Denken anzuregen und mögliche Gefahren abzuwenden.

Inzwischen gibt es einige Unternehmen, die das verstanden haben und den Computerclub nicht bekämpfen, sondern versuchen von seinem Wissen zu profitieren. Das war anscheinend nur eine Frage der Zeit, denn noch vor zwei, drei Jahren wurde der Verein meist noch nicht richtig ernst genommen, während die Mitglieder heute immer öfter zu Vorträgen eingeladen und als Berater angesprochen werden.

Christine Dählmann

((Für einen Kasten:))

Chaos Computerclub e.V. - CCC

Nachdem der Chaos Computerclub e.V. 1981 in Berlin gegründet wurde, gehören ihm inzwischen etwa 200 eingetragene Mitglieder an, von denen allerdings nur 20 - 30 wirklich aktiv sind.
Organisatorisch besteht der Club aus mehreren, selbständigen Gruppen, die ohne einheitliche Führung zusammenarbeiten.

Über Veranstaltungen und Veröffentlichungen (zum Beispiel die Zeitschrift 'Datenschleuder', seit 1984; die 'Hackerfibel' 1 und 2), versucht der CCC über Themen wie Datensicherheit oder Netzwerk- und Computertechnik allgemein, zu informieren.
Der breiten Öffentlichkeit ist der Verein meist nur durch Berichte in den Medien, über gelungene Einbrüche in Computersysteme (beispielsweise der NASA-Hack) und Ereignissen wie der Verhaftung von Steffen Beneri in Paris (März 1988) bekannt.
In seiner Präambel befürwortet der Club den Einsatz von Computern, macht aber auch auf die damit verbundenen Gefahren aufmerksam. Seiner Ansicht nach erfordert die Entwicklung zur 'informierten Gesellschaft', ganz eindeutig ein neues Menschenrecht auf weltweite ungehinderte Kommunikation, weshalb sich die Mitglieder des CCC ausdrücklich für Informationsfreiheit einsetzen.
Sie beschäftigen sich darüberhinaus nicht nur mit den Auswirkungen der neuen Technologien auf die Gesellschaft im allgemeinen und den Einzelnen im besonderen, sondern wollen das Wissen um diese Entwicklungen gezielt fördern.

((Für einen Kasten))

DES - was ist das?

Bei DES - Data Encryption Standard - handelt es sich um einen Verschlüsselungsalgorithmus, der, unter der Federführung von IBM, aus einem anderen Chiffrieralgorithmus heraus entwickelt wurde und in Amerika seit langem als Sicherheitsstandard anerkannt ist.
DES Programme, wie sie zum Beispiel von Bernd Fix vom CCC entwickelt wurden, ermöglichen auf einfache Weise, mit wenig Speicherplatz und zudem bei großer Geschwindigkeit, die Verschlüsselung von

* Dateien und Programmen auf Diskette oder Laufwerk
* Backup-Kopien
* zu übertragenden oder zu übermittelnden Dateien (im Netz oder durch Versendung von Datenträgern).

Ohne das richtige Kodewort (bis 40 Zeichen) ist keinerlei Auswertung von Daten mehr möglich.
Handliche DES Programme sind inzwischen sowohl für PCs, als auch für Datenbanken erhältlich.

Grüß
Eric
15.6.89