Datenschutz in offenen Systemen

Klaus Pommerening
Institut für Medizinische Statistik und Dokumentation
Johannes-Gutenberg-Universität Mainz

1 Einleitung: Datenschutz und Datensicherheit

Daten werden in zunehmendem Maße elektronisch gespeichert und übermittelt, auf Zentralrechnern und Arbeitsplatzrechnern, in öffentlichen und lokalen Netzen. Dabei sind sie vielen Gefahren ausgesetzt: Ausspähung, Verfälschung, Zerstörung. Die Täter hinterlassen kaum Spuren. Der Datenschutz gerät leicht unter die Räder der Computer-Euphorie; insbesondere verstößt die Datenspeicherung auf PC-Systemen nach Ansicht der Datenschutz-Beauftragten in aller Regel gegen Datenschutzbestimmungen.

Auf diesem Symposium wurde das Thema Datenschutz schon einige Male angesprochen. In meinem Übersichtsvortrag geht es um die Vertiefung der praktischen, mehr technischen Aspekte: *Wie* sind die Daten zu schützen? Wo liegen die Gefahren? Wie kann man diese vermeiden oder abmildern? Was kann man selbst tun? Was kann man kaufen? Welche Entwicklungen sind noch von den Herstellern zu fordern?

Daß es zu schützende Daten gibt, steht also quasi als Axiom am Anfang meiner Rede. Sobald auf einem Rechner personenbezogene Daten (oder auch „Betriebsgeheimnisse“) gespeichert sind, müssen auch System- und Anwendungsprogramme geschützt werden, also mehr oder weniger *alle* Daten im System. Die Betreiber eines solchen Systems sind verpflichtet, wirksame Maßnahmen zu treffen, und zwar auf allen Ebenen: organisatorisches Umfeld, Hardware und Software. Für sie sind einerseits Zusammenstellungen der wichtigsten Maßnahmen wichtig, die sie verwirklichen müssen oder können; darüber hinaus brauchen sie auch umfassende Kenntnis von Sicherheitsproblemen, deren Behebung nicht in ihrem Bereich liegt, etwa bei öffentlichen Netzen, bei der Hardware, bei Standard-Software, um die Sicherheit ihres Betriebs beurteilen, Erweiterungen sachgemäß planen und Forderungen an Hersteller stellen zu können. Mit Ignoranz ist kein wirksamer Datenschutz

zu betreiben. In diesem Sinne will ich, soweit das noch nötig ist, Ihren Sinn für Sicherheitsprobleme etwas schärfen.

Das „klassische“ Rechenzentrum ließ sich mit einem gewissen Aufwand an Baumaßnahmen und interner Absicherung zu einem „geschlossenen System“ umwandeln, das hinlängliche Sicherheit bot. Dagegen sind moderne Datenverarbeitungssysteme offen, vernetzt und verteilt; sie sind daher bis auf weiteres unsicher. Wie man mit dieser Unsicherheit umgehen kann, will ich darstellen.

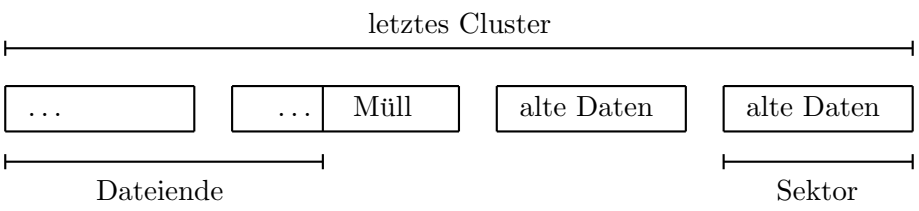
2 Offene Systeme

Doch zunächst will ich an ein paar Beispielen deutlich machen, wie „offen“ die Sorgenkinder der Datenschützer, PCs und Netze, tatsächlich sind.

Beispiel 1: Löschen von Daten. Gelöschte Dateien sind nur im Verzeichnis als gelöscht markiert. In Wirklichkeit stehen die Daten noch da, bis sie irgendwann von anderen Schreibvorgängen überschrieben werden. Bei Festplatten (im Gegensatz zu Disketten) werden die Daten nicht einmal beim gewöhnlichen Formatieren gelöscht. Das Datenschutzgebot „Aufbereitung von Datenträgern zur Wiederverwendung“ ist verletzt. Mit einem Disketten-Monitor wie etwa den „Norton Utilities“ kann man diese Daten leicht sehen, oft sogar ganze gelöschte Dateien wiederherstellen.

Beispiel 2: Schreiben von Daten. Vielleicht wissen Sie, daß das Betriebssystem MS-DOS bzw. PC-DOS bei Schreibvorgängen den freien Raum hinter dem Ende einer Datei bis zum Ende des Clusters mit Daten vollschreibt, die zufällig in einem internen Puffer stehen – das können durchaus Daten sein, die Sie eigentlich geheimhalten wollten, siehe Abbildung 1. Auch diese Daten kann man mit einem Disketten-Monitor leicht sehen.

Abbildung 1: Datenmüll am Dateiende



Beispiel 3: Anschluß von Netzstationen. Sehen Sie irgendwo eine dickes gelbes Kabel liegen, so können Sie einfach eine neue Station an das lokale Netz mit einem „Transceiver“ per ‘Easy Tap Kit’ anschließen und damit einen ‘TAP’ (‘Terminal Access Point’) herstellen. – Werbespruch: „. . . mach(t) Netzwerk-Stops unnötig. Sie zapfen einfach mit dem Easy Tool das Kabel an, schieben den Tap über das Kabel und ziehen fest an. Kein Quetschen oder Löten nötig!“

Beispiel 4: Dataskop oder Schnittstellen-Analysator. Diese Geräte braucht man zur Fehlersuche im Netz. Es gibt sie für Verbindungen aller Art. Man zieht einen Verbindungsstecker ab und stöpselt das Gerät dazwischen. Werbespruch: „. . . nutzen Sie sowohl für die üblichen ‚Kleinigkeiten’, also Pin-Belegung, Brücken oder Baudrate auskundschaften, wie auch für die schwierigeren Fälle

- Datenströme analysieren
- Protokolle und Handshake offenlegen
- Dialoge beobachten
- Leitungen testen
- . . . “

Auch sonst bieten Netze aller Art Abhörmöglichkeiten auf allen Ebenen, mit denen man nicht nur lauschen, sondern zum Teil auch fälschen kann:

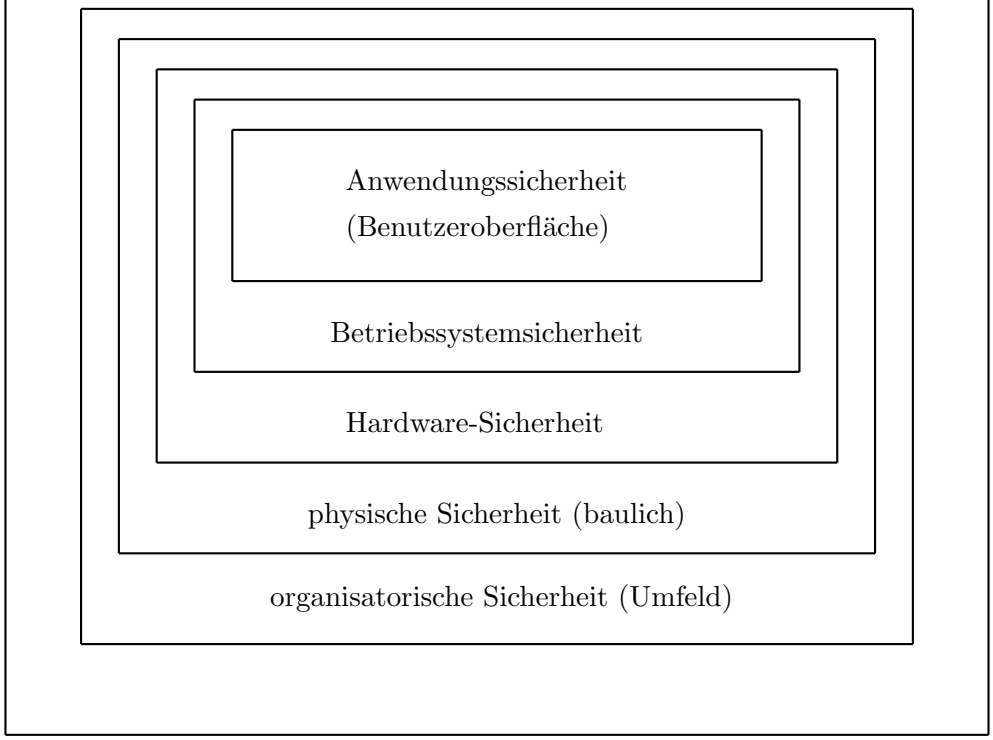
- Elektromagnetische Abstrahlung oder Induktion („Nebensprecheffekt“).
- Anzapfen der Leitung (‘wire tapping’).
- Angriff auf spezielle Kommunikationseinrichtungen wie Modems, Knotenrechner, Brücken.
- Schnittstellen (Stecker raus, Schnittstellentester dazwischen, Stecker wieder rein).
- Besetzung unbenutzter Anschlußpunkte.
- Manipulation regulärer Anschlüsse; denn lokale Netze sind „Diffusionsnetze“ – der gesamte Datenstrom läuft durch jede Station.

In solchen offenen Systemen muß man immer mit dem Zugriff durch Unbefugte rechnen. Auch Viren und andere Schadprogramme können leicht eindringen.

3 Datenschutz in geschlossenen Systemen

Was dagegen ein geschlossenes System ist und wie in ihm die Daten geschützt werden, läßt sich am einfachsten durch ein Schalenmodell verdeutlichen, siehe Abbildung 2.

Abbildung 2: Die Sicherheitsschalen eines geschlossenen Systems



Ist eine der äußeren Schalen durchlässig, so ist der Schutz der inneren Schalen zu umgehen, das System nicht mehr geschlossen. Das verdeutlichen die Beispiele:

1. Die physische Sicherheit, die ein abschließbarer Raum bietet, nützt nichts ohne organisatorische Sicherheit – wenn sich niemand für das Abschließen zuständig fühlt.

2. Die Hardware-Sicherheit durch ein Schloß am PC nützt nichts oh-

ne physische Sicherheit: Man kann den PC einfach wegtragen und zu Hause in aller Ruhe aufbrechen.

3. Die Betriebssystem-Sicherheit eines Paßwortschutzes für die Festplatte nützt nichts ohne eine Hardwaresicherung, die das „Booten“ von einer Diskette verhindert.

4. Die Anwendungs-Sicherheit durch Vergabe von Zugriffsrechten in einem Datenbanksystem nützt nichts, wenn das Betriebssystem gestattet, die Festplatte sektorenweise zu analysieren.

In einem geschlossen System reicht es tatsächlich, Zugriffsrechte auf bestimmte Daten durch Einträge in System-Tabellen zu definieren – das ist eine sichere Maßnahme. Es herrscht das Prinzip der minimalen Rechte und der minimalen Schnittstellen. Die wichtigen Systemkomponenten sind physisch geschützt; auf dieser Grundlage lassen sich logischer Zugang zum System und Zugriff auf Daten wirksam durch das Betriebssystem überwachen. Dieser Schutz ist heute typisch für eine Großrechner-Umgebung.

4 Sicherheitsprobleme im PC-Bereich

Allerdings haben wir es ja meistens mit Arbeitsplatzrechnern (PCs) zu tun. Wenn ein solcher alleinstehend im „Privatbesitz“ ist und in einem nicht frei zugänglichen Raum aufgestellt ist, heißt die wichtigste Sicherheitsmaßnahme:

Rechner abschließen, Disketten wegschließen, Raum zuschließen.

Wenn diese Regel beachtet wird, wird an einem isolierten Arbeitsplatz das Problem des Datenschutzes zwar nicht gelöst, aber durch das Aufstellen des PC auch nicht allzusehr verschärft.

Im Regelfall aber tritt in einer typischen PC-Umgebung eine Reihe von zusätzlichen organisatorischen und technischen Problemen auf (gegenüber großen Datenverarbeitungsanlagen in Rechenzentren):

- Es gibt keine organisatorische Trennung von Systemverwaltung, Bedienung, Programmierung und Anwendung — der Anwender ist Auftraggeber, Programmierer, Operator, Archivar, ... in einer Person.

- Das Betriebssystem ist offen konzipiert und bietet keine Schutzfunktionen. Es gibt wirksame Programme zur Untersuchung von Hauptspeicher und Massenspeichern, mit denen der Zugriff bis zum letzten Bit möglich ist und Schutzmaßnahmen leicht zu unterlaufen sind.

- Die Geräte sind oft unbewacht.
- Ein wirksamer physischer Schutz ist im Vergleich zu den geringen Gerätekosten vergleichsweise teuer und daher nicht wirtschaftlich.
- Die Geräte sind wegtragbar. Ein Angreifer, der einen PC samt Festplatte geklaut hat, hat dann sehr viel Zeit, um vorhandene Schutzmechanismen zu studieren und zu knacken.
- Daten sind leicht auf Disketten zu kopieren und so wegtransportierbar. Auf diskettenlosen Arbeitsplätzen bietet sich als Ersatz an, die Daten auf den Druckerausgang umzulenken. Auch die Hardcopy-Taste ('Prt-Sc') kann zu diesem Zweck dienen, und ihre Verwendung ist kaum zu kontrollieren.
- Gute Systemkenntnisse sind bei möglichen Angreifern weit verbreitet.
- Das Innenleben der Geräte ist leicht zugänglich. Zum Beispiel lassen sich leicht Abhöreinrichtungen („Wanzen") auf Lötkontakte klemmen, mit denen man Paß- und Schlüsselwörter abhören und somit jeden Softwareschutz unterlaufen kann. (Denken Sie auch an den Wartungsdienst – wer hat schon die Zeit, einem Techniker beim Austausch einer Festplatte eine halbe Stunde lang auf die Finger zu schauen.)

Der einzige von den Herstellern vorgesehene Schutz ist das Schloß, das sich an PCs ab der AT-Klasse befindet. Es hält einem Angreifer, der einen Schraubenzieher festhalten kann, allerdings nicht allzu lange stand. Je mehr Benutzer auf dem PC arbeiten, desto unwahrscheinlicher ist es, daß er regelmäßig abgeschlossen wird, falls überhaupt für jeden ein Schlüssel da ist. Seien Sie ehrlich: Schließen *Sie* Ihren PC regelmäßig ab?

Ist der PC in ein Netz eingebunden oder hat er Anschlußmöglickeiten an Großrechner, so ist er nicht nur selbst gefährdet, sondern wird auch umgekehrt zur Gefahrenquelle, wie viele Hacker-Vorfälle gezeigt haben. Eine dieser Gefahren ist die Funktion als „intelligentes Terminal"; der Zielrechner merkt keinen Unterschied zu einem gewöhnlichen „dummen" Terminal. Kommunikationsprogramme erlauben in der Regel, Tastatureingaben durch Programme zu simulieren. So steht einem blitzschnellen Durchprobieren von Tausenden von Paßwörtern nichts im Wege. Eine Gefahr durch berechtigte Benutzer ist, daß sie sich lästige Anmeldeprozeduren automatisieren und dabei auch die Paßwörter mit ins Programm schreiben. Der ersten Gefahr läßt sich mit Maßnahmen auf dem Zielrechner begegnen, gegen die zweite

Gefahr helfen nur organisatorische Maßnahmen – Steigerung des Sicherheitsbewußtseins, Dienstvorschriften, Kontrolle.

5 Verschlüsselungsmethoden

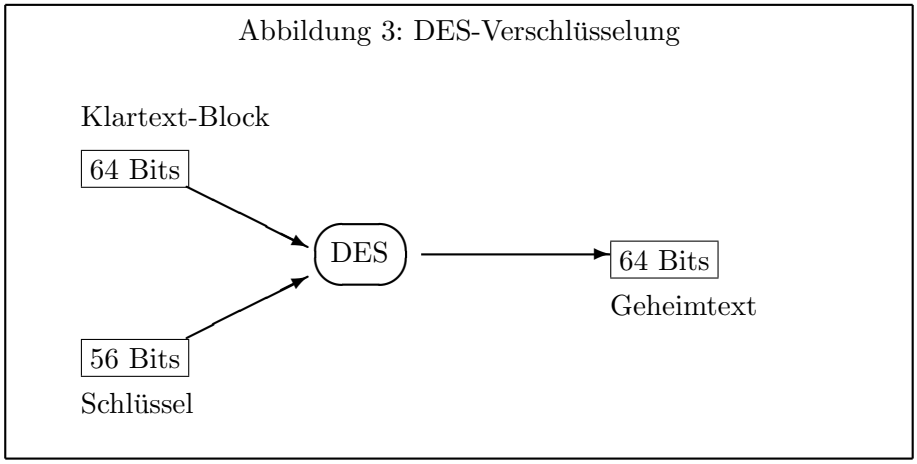
Wenn man das Wort „Kryptographie“, auf deutsch „Geheimschrift“, hört, denkt man zunächst an Geheimdienste, Verschwörungen, Militär, vielleicht auch an Edgar Allen Poe und Schatzsucher. Diese Vorstellungen sind auch nicht falsch – vor allem aber ist Kryptographie heute die wohl wichtigste Grundlage für die Sicherheit der Informationsverarbeitung.

Der Datenschutz in einem geschlossenen System beruht auf der Sicherheit der Umgebung. Anders ausgedrückt: In einer unsicheren Umgebung gibt es keine Sicherheit.

Dies ist aber kein unumstößliches Naturgesetz – genau hier setzt die Kryptographie an: Sie ist die Lehre von der Datensicherheit in einer unsicheren Umgebung. Datenverarbeitungssysteme, die sich nicht physisch sichern lassen, wie etwa große Datennetze, müssen mit kryptographischen Methoden gesichert werden, also durch Verschlüsselung. Verschlüsselung ist auch angebracht auf Datenträgern, die nicht ständig physisch geschützt sind oder deren Diebstahl man fürchten muß.

Die Abbildungen 3, 4 und 5 beschreiben drei wichtige Verschlüsselungsverfahren.

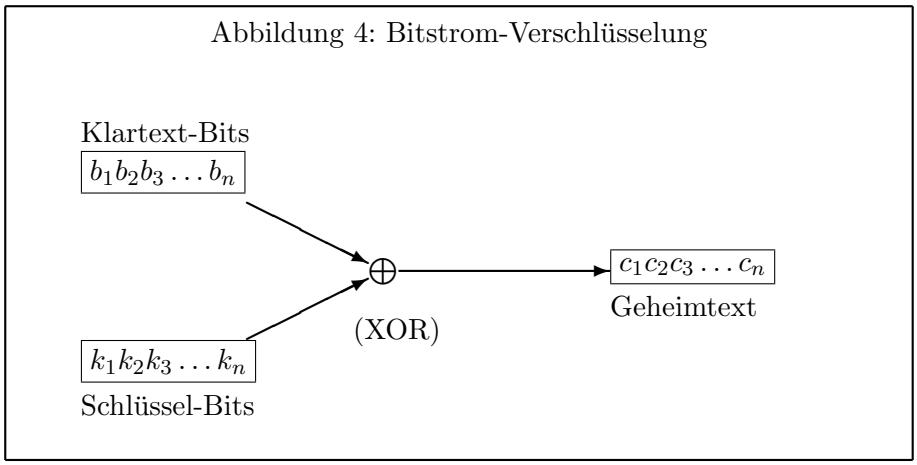
Abbildung 3: DES-Verschlüsselung



Das erste davon ist der **‘Data Encryption Standard’ (DES)**, der 1977

in den USA als Norm definiert wurde. Die Beschreibung ist ziemlich kompliziert (sie besteht aus 3 Seiten voller Tabellen); das Verfahren ist aber leicht in Assembler oder Hardware zu implementieren. DES-Chips verschlüsseln zwischen 0.5 und 20 Mbit/sec, sind also auch für die Datenübertragung in schnellen lokalen Netzen ausreichend. Software-Implementierungen schaffen typischerweise auf einem AT 3 Kbit/sec, und das ist quälend langsam für größere Datenmengen.

Abbildung 4: Bitstrom-Verschlüsselung



Die **Bitstrom-Verschlüsselung** hat den Vorteil besonderer Einfachheit und Schnelligkeit. Leider wird sie, auch in kommerziellen Sicherheitspaketen, oft auf völlig ungenügende Weise verwendet: Es wird einfach ein kurzes Schlüsselwort durch Wiederholung auf die nötige Länge gebracht. Eine solche Verschlüsselung läßt sich durch eine einfache Häufigkeitsanalyse brechen (wie bei Poe). Seien Sie vorsichtig, wenn ein Software-basiertes Verschlüsselungsverfahren 8 KBit/sec oder mehr auf einem AT schafft. Und trauen Sie überhaupt keinem undokumentierten Verfahren. Auf der anderen Seite ist die Bitstrom-Verschlüsselung beweisbar absolut sicher, wenn die Schlüssel-Bits eine echte Zufallsfolge bilden. Daher werden als Kompromiß oft vom Computer erzeugte (Pseudo-) Zufallszahlen genommen. Dann genügt das Verfahren einfachen Ansprüchen, ist aber für Fachleute immer noch (mit etwas Aufwand) zu knacken. Eine ganz neue Erfindung sind „perfekte“ Zufallsgeneratoren, die kryptographisch sichere Pseudozufallszahlen liefern und bei Hardware-Implementation sehr schnell zu machen sind. Meiner Einschätzung nach ist dies das Verschlüsselungsverfahren der Zukunft.

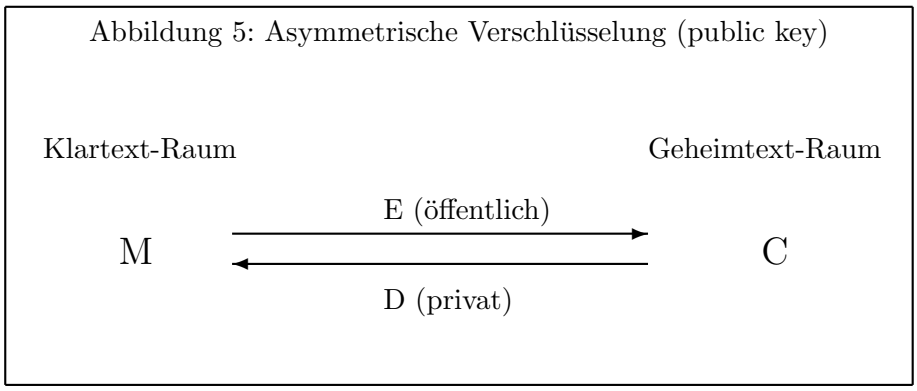


Abbildung 5: Asymmetrische Verschlüsselung (public key)

Bei **asymmetrischer Verschlüsselung** werden zum Verschlüsseln und Entschlüsseln verschiedene Schlüssel verwendet. Der Verschlüsselungsschlüssel wird öffentlich in einer Art Telefonbuch bekanntgegeben; es gibt keine Möglichkeit, aus ihm den geheimgehaltenen privaten Schlüssel zur Entschlüsselung zu bestimmen. Vorteile eines solchen Verfahrens sind:

- Jederzeit spontane Kommunikation mit beliebigen Teilnehmern.
- Keine komplizierten Schlüsselaustausch-Mechanismen nötig.
- Leichte Verwirklichung komplizierter Protokolle.

Das bekannteste Verfahren heißt RSA nach seinen Erfindern Rivest, Shamir und Adleman; seine Sicherheit beruht darauf, daß es keine schnelle Methode gibt, große Zahlen in ihre Primfaktoren zu zerlegen. Leider sind asymmetrische Verfahren vergleichsweise langsam, selbst die schnellsten RSA-Chips schaffen erst 10 – 30 Kbit/sec.

Verschlüsselung allein ist aber noch keine Garantie für Sicherheit. Zum Beispiel sind Schlüssel wie alle Paßwörter gefährdet durch

- Nachlässigkeit des Besitzers,
- ungenügende Schutzvorkehrungen des Systems,
- Abhören von Leitungen, Bildschirmen oder PCs,
- Paßwortfallen,
- systematisches Probieren und Fischzüge.

6 Kryptographische Protokolle

Dürfen wir elektronischen Dokumenten trauen? Die Antwort darauf ist zunächst ein klares „Nein“. Einer der unpassendsten Sprüche, die man immer wieder hört oder liest, ist: „Dieses Dokument wurde von einer elektronischen Datenverarbeitungsanlage erstellt und ist daher ohne Unterschrift gültig.“ Richtig müßte es heißen „. . . und ist daher ohne jede Beweiskraft.“ Nichts ist für Übeltäter leichter, als mit einem Computer jede Menge authentisch aussehenden Papiers zu erzeugen, das dazu noch ein in sich konsistentes Bild bietet. Auch Bilddaten werden zunehmend digital gespeichert, kinderleicht manipulierbar und verlieren dadurch ihren dokumentarischen Charakter.

Betrachten wir das Signaturproblem. Die Teilnehmerin A will dem Teilnehmer B eine Nachricht x zustellen, die niemand fälschen kann. Bei einem asymmetrischen Verfahren nach Abbildung 5 nimmt sie ihren privaten Schlüssel D und bildet $D(x)$. *Niemand sonst* kann $D(x)$ erzeugt haben, *jeder* kann die Echtheit von Text und Unterschrift mit Hilfe des öffentlichen Schlüssels E überprüfen: $x = E(D(x))$. Auch kann A später nicht abstreiten, daß sie selbst es war, die die Nachricht x unterschrieben hat. Entschlüsseln und Signieren sind bei asymmetrischen Verfahren identische Vorgänge – so einfach ist das.

Die primäre Aufgabe der Kryptographie als Wissenschaft ist, Verschlüsselungsmethoden zu entwickeln und ihre Sicherheit gegen unberechtigte Entschlüsselung mathematisch abzusichern. Für den Datenschutz ebenso wichtig ist die weiterführende Aufgabe, für jedes Anwendungsfeld eine geeignete kryptographische Methode zu finden unter der Voraussetzung, daß sichere Verschlüsselungsverfahren existieren. Solche Methoden nennt man **kryptographische Protokolle**.

Unter einem kryptographischen Protokoll versteht man also ein praktisches Verfahren, das ein bestimmtes Sicherheitsproblem löst. Die drei Grundprobleme dieser Art sind:

Chiffrierung – Verschlüsselung, Schutz von Daten gegen unberechtigtes Lesen.

Signatur – elektronische Unterschrift (der Urheber der Daten soll seine Urheberschaft nicht bestreiten können), Schutz von Daten gegen Verfälschung (wobei das Lesen gestattet sein kann oder auch nicht).

Anonymität – der Sender oder Empfänger einer Nachricht soll nicht bekannt werden (gegenüber dritten oder gegenseitig).

Spezielle Ausprägungen dieser Probleme sind: Gegenzeichnung von Dokumenten, Vieraugen- (Mehrschlüssel-) Prinzip, Einschreiben mit Rückschein (= beweissichere Dokumentation von Absendung und Empfang), gegenseitige Identifizierung. Alle diese Probleme lassen sich durch geschickte Kombination von Verschlüsselungsschritten lösen, also durch geeignete kryptographische Protokolle. Am Beispiel der Signatur wurde schon deutlich, welche Möglichkeiten und Chancen für den Datenschutz solche Protokolle bieten können.

Von alledem soll der Endanwender möglichst wenig merken. Daher müssen kryptographische Protokolle, sollen sie routinemäßig angewendet werden, in Hardware und Bertriebssystem verankert sein. Im Alleingang kann man so etwas schon gar nicht implementieren.

Kryptographische Protokolle lassen sich mit symmetrischen und asymmetrischen Verschlüsselungsverfahren verwirklichen, mit asymmetrischen allerdings stets leichter. Die Langsamkeit der asymmetrischen Verfahren stört dabei kaum, da die Protokollsequenzen meist nur aus kurzen Einzelnachrichten bestehen.

Ich betone aber, daß die Umsetzung der Lösungen in die Praxis erst beginnt, einerseits, weil der Weg von der wissenschaftlichen Grundlagenforschung zur alltäglichen Anwendung oft weit ist, andererseits, weil das Sicherheitsbewußtsein der Hersteller und Käufer von Hard- und Software erst langsam erwacht. Findige Hacker haben zur Zeit noch ein weites Betätigungsfeld.

7 Sicherheitskriterien

Für die Entwicklung „offizieller“ Sicherheitskriterien ist in Deutschland das Bundesamt (bis 1990 Zentralstelle) für Sicherheit in der Informationstechnik zuständig. Es hat bisher zwei Schriften herausgegeben:

- IT-Sicherheitskriterien.
- IT-Evaluationshandbuch.

Beide sind im Bundesanzeiger-Verlag erschienen und kosten je um die 10 DM. Da vor allem das zweite sehr leicht verständliche Beispiele enthält, sind sie als Lektüre für Sicherheitsverantwortliche durchaus zu empfehlen. Sie definieren Grundfunktionen der Informationssicherheit, Mechanismen und deren Stärke, Funktionalitätsklassen und Qualitätsstufen. Der Sinn eines solchen Kriterienkatalogs ist:

- Vertrauenswürdigkeit von Datenverarbeitungssystemen definieren.
- Standards für Systemhersteller setzen; allgemeine Hebung des Sicherheitsstandards; Qualitätsdruck auf die Hersteller.
- Beurteilungsmaßstäbe für Betreiber und Anwender zur Verfügung stellen; Hilfe bei der Erstellung von Ausschreibungen.
- Prüfrichtlinien für offizielle Bewertungsstellen („objektive Vertrauensbildung“ durch „neutrale und vertrauenswürdige Institution“).

Nach der Etablierung entsprechender Standards sollte folgendes Vorgehen bei der Installation eines vertrauenswürdigen Datenverarbeitungssystems möglich sein:

1. Risikoanalyse (organisorisches Umfeld, Datenmodell, einzusetzende Verarbeitungsverfahren).
2. Anforderungsdefinition (Funktionalitäts- und Qualitätsanforderungen nach den Maßstäben des Kriterienkatalogs).
3. Auswahl eines entsprechend klassifizierten Systems.

Es sollte so auf lange Sicht überflüssig werden, daß jeder Systembetreiber die letzten Winkel seines Systems kennen muß, um wirksame Schutzmaßnahmen durchführen zu können.

8 Sicherheitsprodukte

Die wichtigste Klasse von Sicherheitshardware für offene Systeme bilden Verschlüsselungs-Chips. Verschlüsselung von Daten kostet Rechenzeit; wenn möglich sollte man dafür gesonderte Einsteckkarten verwenden, die einen eigenen Prozessor mit RAM-Speicher und den Algorithmus in einem ROM haben. Eine Verschlüsselungskarte läßt sich zu einem brauchbaren Sicherheitssystem für den PC ausbauen. Sie kann zum Beispiel einen nicht zu umgehenden Paßwortschutz gewährleisten, eventuell gekoppelt mit einem mechanischen Schlüssel. Damit man die Karte nicht einfach ausbauen kann, sollte sie mit einem Selbstzerstörungsmechanismus versehen sein, etwa einem Lichfenster im ROM, das für dessen Löschung sorgt, indem beim Abhebeln eines Verschlusses eine Fotozelle ausgelöst wird. Ferner sollten Lötstellen nicht zugänglich sein, damit nicht an ihnen Informationen abgezapft werden können. Auf der Basis einer solchen Karte läßt sich eine hohe

Systemsicherheit verwirklichen. Benutzerverwaltung, Kopien auf Diskette, Formatieren der Festplatte, Änderungen an der Systemkonfiguration, etwa die Einstellung der Zeit, und andere sicherheitsrelevante Prozeduren werden verhindert, wenn sie nicht von besonders berechtigten Personen vorgenommen werden. Drucker, Diskettenlaufwerke und andere Peripheriegeräte können gezielt für einzelne Benutzer gesperrt werden. Auch andere Schutzmaßnahmen aus dem Bereich der geschlossenen Systeme lassen sich so auf den PC übertragen.

Ohne Verschlüsselung ist echter Datenschutz auf dem PC nicht möglich, da nicht verhindert werden kann, daß ein Anwendungsprogramm volle Kontrolle über die CPU bekommt und somit auf der untersten Maschinenebene, noch unterhalb des Betriebssystems, alle Ein-und-Ausgabemedien ansprechen kann.

Für den Zeitpunkt der Verschlüsselung der Daten auf der Festplatte gibt es zwei Konzepte: Das einfachere ist, daß Dateien vor der Bearbeitung entschlüsselt und nach der Bearbeitung wieder verschlüsselt werden. Das behindert bei der eigentlichen Arbeit dann zwar nicht mehr, muß aber in der Regel von Hand ausgeführt werden, so daß sich der Arbeitsbeginn verzögert, und am Ende steht die Gefahr, daß man das Wiederverschlüsseln vergißt. Eine andere Lösung ist, daß die Daten während der Bearbeitung, also auf dem Weg zwischen Platte und Hauptspeicher ent- oder verschlüsselt werden ('online'). Die Verschlüsselung ist zeitraubend, wenn sie per Software realisiert wird – und gerade die wichtigen Daten sind die, die man ständig braucht; für 'online'-Verschlüsselung muß das Verfahren dann in einem Gerätetreiber installiert sein. Wird es dagegen per Hardware erledigt, ist es teuer. Auch sind nicht alle auf dem Markt angebotenen Verschlüsselungsverfahren so einbruchsicher, wie es die Werbung verheißt. Dazu kommt, daß man sich ein Schlüsselwort merken muß (sonst taugt das Verschlüsselungsverfahren garantiert nichts), und damit beginnen die die üblichen Paßwortprobleme.

Trotz aller Vorbehalte können auch einfache Verschlüsselungsprogramme wertvoll sein, wenn man nicht mit professionellen Angreifern rechnen muß. Sie schützen davor, daß geschützte Daten versehentlich offengelegt werden, etwa wenn eine Diskette auf dem Transport verloren geht. Auch die Festplatte eines PCs kann im Falle eines Hardware-Diebstahls so durchaus ausreichend geschützt sein. Verschlüsselte Programme sind übrigens auch gegen die Einnistung von Viren gefeit; ein Virus kann sich zwar ins Programm kopieren, bei der Entschlüsselung wird es aber in „Bytesalat“ verwandelt.

Ein weiterer Typ von Schutzprogrammen soll vor unbefugten Datenveränderungen schützen; diese werden meist in der Kategorie „Anti-Virus-

Programme“ verkauft. Das Prinzip ist, Daten und Programme, auch die Systemspuren auf der Festplatte, regelmäßig auf Änderungen zu untersuchen, wobei meistens eine Prüfsumme mit einem Sollwert verglichen wird. Dieses Verfahren kann natürlich nur wirken, wenn der Angreifer es nicht so gut kennt, daß er es austricksen kann. Andere Programme, die zum Virenschutz angeboten werden, suchen nach bekannten Viren oder verhindern deren Verbreitung. Gegen neue Viren helfen sie natürlich nicht.

In die Kategorie Sicherheitshardware gehören abgeschirmte Terminals und Kommunikationsleitungen sowie einmal beschreibbare optische Platten ('WORM') zur manipulationsgeschützten Protokollierung von Vorgängen. Wechselbare Festplatten erlauben, auch größere Datenbestände sicher aufzubewahren. Andererseits haben Arbeitsplatzrechner ohne Diskettenlaufwerk in einem Netz den Vorteil, daß Daten nicht so leicht unbefugt wegtransportiert werden können. Außerdem lassen sich nicht so leicht Viren ins System kopieren. Das Umlenken von Ausgabedaten auf einen Drucker wird allerdings nicht verhindert.

Einfache Magnetkarten-Systeme bieten in den meisten Anwendungsfällen keine ausreichende Sicherheit. Wer einen PC hat und zusätzlich etwa 5000 DM für ein Kartenlese- und -schreibsystem mit passender Software anlegt, kann Magnetkarten beliebig kopieren oder ändern. Deutlich erhöhte Sicherheit bietet dagegen ein neuer Typ von maschinenlesbaren Ausweiskarten, die Chip-Karten, die zusätzlich durch ein Paßwort („PIN“) geschützt sind. Die Chipkarte als Zugangskontrollsystem eröffnet neue Möglichkeiten, den Datenschutz zu verbessern.

Es gibt eine Reihe von fertigen Sicherheitsprodukten auf dem Markt, die je nach organisatorischer Umgebung, physischen Schutzmöglichkeiten und Schutzbedürftigkeit der Daten die Datensicherheit auf einem PC wesentlich verbessern können und ein beträchtliches Sicherheitsniveau ermöglichen. Gute Produkte kosten zur Zeit einiges über 1000 DM und einige Mühe für die Einarbeitung und laufende Verwaltung. Sie bestehen teils aus Hardwarekomponenten, teils aus Software; am sichersten ist die Kombination von beidem.

Auch für Netze gibt es inzwischen einiges an Sicherheitshardware, etwa das IBM-Transaktionssicherheitssystem, das einen Netzwerk-Sicherheitsprozessor, einen kryptographischen Adapter und eine Sicherheits-Zugangseinheit enthält. Es gibt Chiffrier-Modems und Chiffriereinrichtungen für Datex-P-Anschlüsse. Für die Zukunft wichtig ist das Netz-Sicherheitssystem 'Kerberos', das am MIT ('Project Athena') entwickelt wird.

9 Kosten und Nutzen des Datenschutzes

Datenschutz verursacht Kosten. Das können direkte Kosten für bauliche Maßnahmen oder zusätzliche Software sein oder Kosten für zusätzliches Personal mit Sicherheitsaufgaben. Kosten entstehen aber auch indirekt in Form von Zeit und Mühe. Zeit braucht man für die Planung, aber auch im täglichen Umgang mit den Sicherheitsmaßnahmen. Mühe verursachen die ständig geforderte Aufmerksamkeit oder lästige Identitätskontrollen. Nicht zu vergessen ist auch, daß einige Schutzmaßnahmen wie die Verschlüsselung oder die Überprüfung von Zugriffsberechtigungen auf Datenfeld-Ebene Datenverarbeitungsleistung kosten und die Antwortzeiten am Terminal erhöhen.

Demgegenüber sind der Wert der zu schützenden Daten und Informationen, die Wahrscheinlichkeit eines Schadensfalls und der Verlust, der im Schadensfall entsteht, abzuwägen. Der Wert der Daten ist nicht notwendig materiell bestimmbar, wie das Beispiel von personenbezogenen Daten, etwa Patientendaten im Krankenhaus oder Personaldaten im Betrieb, zeigt. Hier ist unabhängig von Kostengesichtspunkten der nach dem Stand der Technik mögliche und nach dem Ausmaß der Bedrohung nötige Schutz zu leisten. Natürlich ist auch das Prinzip der Verhältnismäßigkeit im Auge zu behalten; militärische Sicherheitsmaßnahmen sind in einem Krankenhaus wohl nicht angebracht.

Kosten-Nutzen-Abwägungen sind auch aus dem Blickwinkel des potentiellen Angreifers durchzuführen. Lohnt es sich für ihn, den Aufwand zur Überwindung der Schutzbarrieren auf sich zu nehmen? Ein typisches Beispiel für eine solche Überlegung ist die Bestimmung des Aufwands zum Entschlüsseln verschlüsselter Daten. Die Kosten für den Angreifer sind auch wieder nicht nur materiell zu sehen; die Gefahr, entdeckt zu werden, gehört ebenfalls dazu. Erschwert wird die Rechnung dadurch, daß sein Nutzen die Befriedigung nichtmaterieller Bedürfnisse sein kann, für die ihm kaum ein Aufwand zu hoch ist.

Bei der Abwägung von organisatorischen Maßnahmen statt eingebauter Schutzmechanismen ist zu bedenken, daß organisatorische Maßnahmen (z. B. Verbote) zwar oft wenig kosten, aber mit der wachsenden Komplexität der Systeme auch immer unübersichtlicher und schwerer zu überwachen werden und von der Zuverlässigkeit der Mitarbeiter abhängen. Die Kosten für systeminterne Schutzmechanismen sinken durch den Preisverfall der Hardware, der immer weiteren Verfügbarkeit von Standard-Software-Lösungen und der immer größeren Leistungsfähigkeit der Systeme, die einen Leistungsverlust durch Schutzmaßnahmen verschmerzbar macht.

Sicherheitsmaßnahmen kann man grob einteilen in

einfache Maßnahmen – sie schützen vor versehentlichen Einblicken und verdeutlichen dem gutwilligen Benutzer des Systems, wo seine Befugnisse enden.

mittelstarke Maßnahmen – sie sind nur mit Spezialausrüstung oder Spezialkenntnissen zu durchbrechen.

sichere Maßnahmen – sie sind nach dem Stand der Technik mit den existierenden Ressourcen nicht zu durchbrechen.

Eine einfache Maßnahme ist zum Beispiel ein Paßwortsystem für eine PC-Festplatte; sie kann durch „booten“ von einer Diskette umgangen werden. Eine mittelstarke Maßnahme ist der Paßwortschutz auf einem geschlossenen System, sofern er mit einer geeigneten Überprüfung verbunden ist, die etwa Trivialpaßwörter verhindert. Als sichere Maßnahme darf man die Verschlüsselung mit DES oder RSA betrachten.

10 Zusammenfassung

- Vertrauen auf Unwissenheit ist keine Datenschutzmaßnahme.
- Soweit möglich sollte man ein geschlossenes System anstreben, insbesondere für physischen Schutz sorgen.
- Daten lassen sich in offenen Systemen wirksam schützen, wenn, aber auch nur wenn, man kryptographische Methoden anwendet.
- Verschlüsselung ohne Hardware-Unterstützung ist in der Regel zu langsam; es gibt aber auf dem Markt sehr gute Sicherheitssysteme, die auf Verschlüsselungs-Chips basieren.
- Kryptographische Protokolle sind nicht vom Endanwender in Eigenregie einführbar; die Hersteller offener Systeme sind in der Pflicht, wirksame Implementierungen anzubieten.
- Für Systeme in Klinik und ärztlicher Praxis sind geeignete technische Standards wünschenswert, die man den Herstellern gegenüber durchsetzen kann.

Literatur

[1] Thomas A. Berson, Thomas Beth (eds.): *Local Area Network Security.* Workshop LANSEC '89, Karlsruhe FRG, April 1989, Lecture Notes in Computer Science, Springer Verlag, Berlin 1989.

[2] Albrecht Beutelspacher: *Kryptologie.* Vieweg, Braunschweig 1987.

[3] Der Bundesbeauftragte für den Datenschutz (Hrsg.): *Bürgerfibel Datenschutz.* Bonn 1980.

[4] David Chaum: Security without identification: Transaction systems to make Big Brother obsolete. Communications of the ACM 28 (1985), 1030–1044.

[5] Datenschutzkommission Rheinland-Pfalz: *Datenschutzrechtliche Anforderungen an wissenschaftliche Forschungsvorhaben.* Informationen zum Datenschutz, Heft 3, Mainz 1987.

[6] Dorothy Elizabeth Robling Denning: *Cryptography and Data Security.* Addison-Wesley, Reading Mass. 1982.

[7] Winfried Gleißner, Rüdiger Grimm, Siegfried Herda, Hartmut Isselhorst: *Manipulation in Rechnern und Netzen.* Addison-Wesley, Bonn usw. 1989.

[8] Lance J. Hoffman (ed.): *Rogue Programs: Viruses, Worms, and Trojan Horses.* Van Nostrand Reinhold, New York 1990.

[9] IBM: *Communications Security: "In-House" Cable and Line Considerations.* Document Number ZZ81-0232, December 1989.

[10] David R. Johnson, Thomas P. Olson, David G. Post: *White Paper on Computer Viruses.* American Council on Education and United Educators Insurance, 1989.

[11] Hans-Albert Lennartz: *Datenschutz und Wissenschaftsfreiheit.* DuD-Fachbeiträge 10, Vieweg, Braunschweig 1989.

[12] Computer – Chaos machbar. Der Spiegel 25/1989, 185–186.

[13] Peter Paul Spies (Ed.): *Datenschutz und Datensicherung im Wandel der Informationstechnologien.* 1. GI-Fachtagung, München, Oktober

1985, Proceedings, Informatik-Fachberichte 113, Springer-Verlag, Berlin usw. 1985.

[14] Gerhard Weck: *Datensicherheit.* Leitfäden der angewandten Informatik, B. G. Teubner, Stuttgart 1984.

[15] Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): *IT-Sicherheitskriterien – Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT).* Bundesanzeiger, Köln 1989.

[16] Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): *IT-Evaluationshandbuch – Handbuch für die Prüfung der Sicherheit von Systemen der Informationstechnik (IT).* Bundesanzeiger, Köln 1990.