in: Hans-Werner Moritz, Thomas Dreier (Hg.): Rechts-Handbuch zum E-Commerce, Verlag Dr. Otto Schmidt KG, Köln 2002, 805-817.

F. Sicherheit im Netz

1. Datensicherheit

1.1 Abgrenzung von Datensicherheit und Datenschutz

In komplexen IT-Systemen, wie es unsere heutigen und zukünftigen Kommunikationsnetze sind, handeln verschiedene Subjekte (Organisationen, Personen). Sie können dabei nicht nur kooperieren, sondern auch konkurrieren (z. B. um Betriebsmittel), sabotieren (z. B. Kommunikation behindern, stören, blockieren, lahmlegen), fingieren (z. B. Identitäten vortäuschen, Daten verändern) oder abhören (z. B. bespitzeln, lauschen). Die Großrechner vor 20 Jahren waren streng bewacht, d.h. für sie galten Zugangskontrollmaßnahmen (Pförtner, Stahltüren etc.), die nicht leicht zu überwinden waren. Die Vernetzung von Rechnern blieb Spezialanwendungen vorbehalten.

Während **Datensicherheit** die Daten schützen soll, schützt **Datenschutz** die Menschen. Datensicherheit betrifft den Schutz von Daten vor Mißbrauch, (Ver)-Fälschung und Verlust bzw. Nicht-Verfügbarkeit. Datenschutz betrifft dagegen den Gebrauch von personenbezogenen Daten durch Berechtigte. Datenschutz ist primär aus der Sicht des Betroffenen interessant, während Datensicherheit primär aus der Sicht des Datenverarbeiters und -besitzers betrachtet wird.

1.2 Bedrohungen und Schutzziele

IT-Systeme (einschließlich der Übertragungsstrecken) müssen dazu gegen unbeabsichtigte Fehler und Ereignisse (z. B. höhere Gewalt, technische Fehler, Fahrlässigkeit, Programmierfehler, Verschleiß, Havarien) und beabsichtigte Angriffe (z. B. Abhören, Manipulation und Zerstören von Informationen, aber auch von Software und Hardware) von außen (z. B. Hacker oder Terroristen mit Sprengstoff) und innen (z. B. Administratoren, Programmierer) gesichert werden.

Im Englischen werden die Begriffe *security* für den Schutz vor beabsichtigten und *safety* für den Schutz vor unbeabsichtigten Ereignissen verwendet (Tabelle 1).

Security Schutz gegen beabsichtige Angriffe		Safety Schutz gegen unbeabsichtigte Ereignisse	
Vertraulichkeit:	Anonymität Unbeobachtbarkeit Unverkettbarkeit Pseudonymität Abhörsicherheit Sicherheit gegen unbefugten Gerätezugriff	Verfügbarkeit:	Funktionssicherheit Technische Sicherheit
Integrität:	Unabstreitbarkeit Übertragungsintegrität Abrechnungssicherheit Übertragungssicherheit	Sonstige Schutzziele:	Maßnahmen gegen hohe Gesundheitsbelastung
Verfügbarkeit:	Ermöglichen von Kommunikation		
Abwehr der Angriffe gegen Insider und Outsider			

Tabelle 1. Abgrenzung von Security und Safety

Seit den frühen 80er Jahren[1] findet sich eine Dreiteilung der Bedrohungen und korrespondierenden **Schutzziele** Vertraulichkeit, Integrität und Verfügbarkeit:

- Unbefugter Informationsgewinn, d.h. Verlust der **Vertraulichkeit** (Confidentiality),
- Unbefugte Modifikation von Informationen, d.h. Verlust der **Integrität** (Integrity) und
- Unbefugte Beeinträchtigung der Funktionalität, d.h. Verlust der **Verfügbarkeit** (Availability).

Die neuen Kommunikationsmedien sollen zunächst natürlich erwünschte Funktionen leisten, allerdings ebenso unerwünschte Funktionen oder Verhaltensweisen verhindern. Entsprechend lassen sich die großen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit verfeinern.

	Inhalte Worüber?	Umfeld Wer, wann, wo, mit wem, wie lange?
Unerwünschtes verhindern	Vertraulichkeit von Nachrichteninhalten	gegenseitige Anonymität der Anwender; Unbeobachtbarkeit der Anwender durch die Betreiber
Erwünschtes leisten	Integrität von Nachrichteninhalten	Zurechenbarkeit von Nachrichten zu Absendern und/oder Empfängern
	Verfügbarkeit von Daten und Diensten	Erreichbarkeit von Anwendern

Tabelle 2. Gliederung von Schutzzielen

Schutzinteressen können sich nicht nur auf die über die Netze ausgetauschten Nachrichteninhalte (Vertraulichkeit, Integrität) beziehen, sondern gelten ebenfalls für den Schutz von **Kommunikationsumständen**: In manchen Anwendungen ist zu schützen, wer wann mit wem kommuniziert hat (Anonymität und Unbeobachtbarkeit), in anderen Anwendungen ist vor allem sicherzustellen, daß eine Nachricht nachprüfbar und beweisbar von einem bestimmten Absender stammt und/oder einen Empfänger nachweisbar erreicht (Zurechenbarkeit).

Die Vertraulichkeit von Nachrichten kann mit Hilfe von **Verschlüsselung** erreicht werden.

Message Authentication Codes dienen dem Schutz von Nachrichten vor unerkannter Verfälschung auf den Übertragungswegen.

[1] Viktor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; ACM Computing Surveys 15 (1983), No. 2, June 1983, 135-170.

Mit Hilfe der **digitalen Signatur** ist Zurechenbarkeit realisierbar: Nachrichten können so ihrem „Unterzeichner“ eindeutig zugeordnet werden.

Die Anonymität und Unbeobachtbarkeit von Internet-Nutzern kann durch sog. **datenschutzfreundliche Techniken** realisiert werden. Im Bereich E-Commerce sind die bekanntesten Verfahren, die zur Klasse der anonymen Verfahren zählen, die digitalen anonymen Zahlungssysteme[2] und Verfahren zum unbeobachtbaren Web-Surfen im Internet[3].

Die Verfügbarkeit von Daten und Diensten kann erreicht werden durch **Diversität und redundante Auslegung** von Leitungskapazitäten, Rechenressourcen und Datenspeichern.

Angreifermodell

Die Schutzmechanismen, die die Schutzziele implementieren, schützen vor einem Gegner bis zu einer bestimmten Stärke, die im Angreifermodell definiert wird. Ein **Angreifermodell** definiert die Stärke eines Angreifers, gegen den ein bestimmter Schutzmechanismus (z.B. ein ganz bestimmtes Verschlüsselungsverfahren) gerade noch sicher ist. Dabei berücksichtigt es folgende Aspekte:

1. Aktive oder passive Rolle des Angreifers:
   - Was kann der Angreifer maximal passiv beobachten?
   - Was kann der Angreifer maximal aktiv kontrollieren (steuern, verhindern) bzw. verändern?
2. Mächtigkeit des Angreifers:
   - Wieviel Rechenkapazität besitzt der Angreifer?
   - Wieviel finanzielle Mittel besitzt der Angreifer?
   - Wieviel Zeit besitzt der Angreifer?
   - Welche Verbreitung hat der Angreifer? Oder spezieller: Welche Leitungen, Kanäle, Rechner kann der Angreifer beherrschen?

Als potentielle Angreifer können Außenstehende, Teilnehmer, Betreiber, Hersteller, Entwickler und Wartungstechniker betrachtet werden, die natürlich auch kombiniert auftreten können. Außerdem kann man nach Angreifern innerhalb des betrachteten IT-Systems (Insider) und außerhalb (Outsider) unterscheiden. Die Feststellung, daß eine Instanz angreifen kann, ist nicht gleichzusetzen damit, daß sie wirklich angreift.

Die Vertrauensverhältnisse zwischen den verschiedenen beteiligten Instanzen innerhalb eines IT-Systems entscheiden stark darüber, welches Schutzniveau für den einzelnen Beteiligten tatsächlich erreicht werden kann. Nicht selten gilt dabei, wie im „wirklichen Leben“, daß die Mächtigen ihre Interessen gegen die schwächeren Partner durchsetzen, zumindest solange sie dies auf legaler Basis tun können. Man könnte diesen Prozeß mit dem evolutionären Grundgedanken, daß der (genetisch) Stärkere den Überlebenskampf gewinnt, erklären und billigen. Glücklicherweise hat sich aber in den letzten Jahren eine Gegenströmung im Bereich der IT-Sicherheit etabliert, die dieser einseitigen Betrachtung von Sicherheit und Schutz das Konzept der mehrseitigen Sicherheit entgegenstellt.

Mehrseitige Sicherheit

Mehrseitige Sicherheit[4,5] bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung. Dabei gilt:

---

[2] Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

[3] Hannes Federrath, Andreas Pfitzmann: Neue Anonymitätstechniken. Datenschutz und Datensicherheit DuD 22/11 (1998) 628-632.

[4] Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997.

- Jeder Beteiligte hat Sicherheitsinteressen.
- Jeder Beteiligte kann seine Interessen formulieren.
- Konflikte werden erkannt und Lösungen ausgehandelt.
- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.

Die Realisierung von mehrseitiger Sicherheit führt nicht zwangsläufig dazu, daß die Interessen aller Beteiligten erfüllt werden. Sie gewährleistet jedoch, daß die Partner einer mehrseitig sicheren Kommunikation in einem geklärten Kräfteverhältnis bzgl. Sicherheit miteinander interagieren.

Die mehrseitige Sicherheit verbindet die Sichtweisen von Datenschutz und Datensicherheit zu einem gemeinsamen Konzept. Während sich Datenschutz hauptsächlich um die Interessen der Betroffenen kümmert und Datensicherheit vor allem die Interessen der Datenbesitzer und –verarbeiter beachtet wird bei mehrseitiger Sicherheit in einem Aushandlungsprozeß versucht, möglichst beides, Datenschutz und Datensicherheit zu gewährleisten. Dies trägt der Entwicklung Rechnung, dass aus den bisher lediglich Betroffenen zunehmend informationstechnisch Beteiligte werden können und oftmals werden sollten.

1.3 Physische Sicherheit

Um sichere Kommunikation zu erreichen, werden Geräte (Hardware) und Programme (Software) benötigt, die für denjenigen, der sie benutzt, sicher sind. Diese persönliche Rechenumgebung (typischerweise der PC) ist der **Vertrauensbereich** des Benutzers: Es wird angenommen, daß Angriffe auf die Interessen des Benutzers innerhalb dieses Bereiches nicht stattfinden. In diesem Vertrauensbereich kann der Nutzer Berechnungen integer und ggf. vertraulich durchführen. Darüber hinaus muß das Gerät auch über ein vertrauenswürdiges Benutzungsinterface verfügen. Ist ein Benutzerendgerät für den Teilnehmer nicht (mehr) vertrauenswürdig, so können noch so gute kryptographische Systeme ihm keinerlei vertrauenswürdige Sicherheit bieten.

Der Vertrauensbereich ist vor Zugang und Zugriff durch Unberechtigte zu schützen. Dies muß zunächst durch physische Schutzmaßnahmen (Zugangskontrolle) erfolgen, bevor weitere Maßnahmen wie Zugriffskontrolle sinnvoll sind.

Dies betrifft zunächst den persönlichen Rechner zu Hause und am Arbeitsplatz. In den heute weit verbreiteten PC-Betriebssystemen (DOS, Windows 95/98/ME/CE, MacOS) fehlt leider die Zugriffskontrolle, so daß der Ausbreitung von Viren und trojanischen Pferden Tür und Tor geöffnet ist. Leider sind aber auch weniger unsichere Betriebssysteme wie Windows NT und Windows 2000 mit Zugriffskontrolle in ihren inneren Funktionen vom Hersteller nicht genug offengelegt, um sie wirklich prüfen und ihnen danach ggf. vertrauen zu können. Die Existenz Trojanischer Pferde kann somit nicht völlig ausgeschlossen werden. Trojanische Pferde können nicht nur die Vertraulichkeit von privaten oder geschäftlichen Geheimnissen verletzen; sie sind in der Lage, alle Schutzziele, also auch Integrität und Verfügbarkeit zu verletzen. Im schlimmsten Fall kann ein Trojanisches Pferd seine Schadensfunktion modifizieren und sich so an seine aktuelle Umgebung anpassen und sogar sich selbst zerstören, nachdem es seine Aufgabe erfüllt hat, um keine Spuren zu hinterlassen.

Alle technischen Schutzmaßnahmen benötigen also eine physische „Verankerung“ in Form eines Systemteils, auf den der Angreifer keinen physischen Zugriff hat.

Beispielsweise ist es unmöglich, den Inhalt einer zu verschlüsselnden Nachricht vor dem Verschlüsselungsbaustein zu verbergen. Dies gilt analog für die eingesetzten kryptographischen Schlüssel.

Die Größe physisch sicherer Geräte muß skalierbar sein, d.h. ein Vertrauensbereich ist nicht notwendigerweise deckungsgleich mit dem PC (Abbildung 1).

---

[5] Günter Müller, Kai Rannenberg (Ed.): Multilateral Security in Communications, Addison-Wesley-Longman 1999.

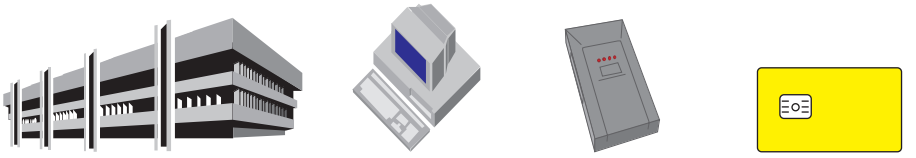

Abbildung 1. Die Größe physisch sicherer Geräte muß skalierbar sein

Beispiel: Es soll der Inhalt einer Festplatte vor unbefugtem Zugriff geschützt werden. Um zu verhindern, daß die Festplatte aus dem Rechner ausgebaut wird, muß der Rechner physisch sicher sein. Alternativ kann die Festplatte verschlüsselt werden. Die Ver- und Entschlüsselung der Festplatte erfolgt über ein Sicherheitsmodul, das während des Betriebs im Rechner steckt. Nun genügt es, daß das Sicherheitsmodul physisch geschützt wird. Wird der Rechner bzw. die Festplatte gestohlen, bleiben die gespeicherten Inhalte trotzdem vertraulich.

Die maximal erreichbare persönliche Sicherheit eines Benutzers eines IT-Systems kann – bezogen auf das IT-System – nie größer werden als die Sicherheit des Gerätes, mit dem er physisch direkt interagiert.

Angriffe auf die physische Sicherheit werden, unabhängig von der jeweiligen Größe des physischen Gerätes, durch Schirmung (z.B. gegen elektromagnetische Abstrahlung), Erkennen und Bewerten (z.B. durch entsprechende Sensoren) sowie Verzögern des Angriffs (z.B. durch hartes Material) realisiert. Bei Angriffen können als letzte Maßnahme die gespeicherten Geheimnisse gelöscht werden.

Die Realisierung eines physisch sicheren und für den Benutzer vertrauenswürdigen Endgerätes ist kein triviales Problem[6,7] und gelingt bestenfalls auf Zeit, da immer wieder neue Angriffe auf vermeintlich sicher geglaubte physisch sichere Geräte (z.B. Chipkarten) bekannt werden.

1.4 Zugangskontrolle

Unter **Zugangskontrolle** versteht man, daß ein IT-System die Identitäten seiner Kommunikationspartner erfragt, prüft und nur mit berechtigten Partnern weiter kommuniziert.

Die Zugangskontrolle verhindert so mindestens die unbefugte Inanspruchnahme seiner Betriebsmittel. Ein IT-System kann einen Menschen daran erkennen (**Identifikation**), was er ist, hat oder weiß (Tabelle 3).

[6] Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trusting Mobile User Devices and Security Modules. Computer 30/2 (1997) 61-68.

[7] Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule. Hans H. Brüggemann, Waltraud Gerhardt-Häckl (ed.): Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS '95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 329-350.

Was man…		
…ist:	**…hat:**	**…weiß:**
• Handgeometrie • Fingerabdruck • Aussehen • Eigenhändige Unterschrift • Retina-Muster • Stimme • Tipp-Charakteristik (Tastenanschlag) • DNA-Muster	• Papierdokument • Metallschlüssel • Magnetstreifenkarte • Chipkarte • Taschenrechner	• Passwort • Antworten auf Fragen

Tabelle 3. Identifikation von Menschen durch IT-Systeme

Beispiele: 1. Ein (maschinenlesbarer) Personalausweis ist eine Kombination aus Foto („Aussehen“), eigenhändiger Unterschrift und Papierdokument. 2. Die in IT-Systemen derzeit noch am häufigsten vorkommende Form der Identifizierung ist das Passwort.

1.5 Zugriffskontrolle und Rechtevergabe

Unter **Zugriffskontrolle** versteht man, daß ein IT-System auch berechtigten Partnern nicht alles erlaubt: Jedes *Subjekt* (Mensch, IT-System, Prozeß) hat nur bestimmte *Rechte*, Operationen auf *Objekten* (Prozesse, Daten, Peripherie-Geräte, etc.) auszuführen.

Ein möglichst kleiner und gut abgegrenzter Teil des IT-Systems kontrolliert vor Ausführung aller Operationen, ob ihr Urheber die dafür nötigen Rechte hat. Dieser Teil des IT-Systems wird **Zugriffsmonitor** genannt (Abbildung 2). Der Zugriffsmonitor merkt sich ihm vorgelegte oder implizit entstehende Rechte und muß auch deren Ungültigwerden erkennen.

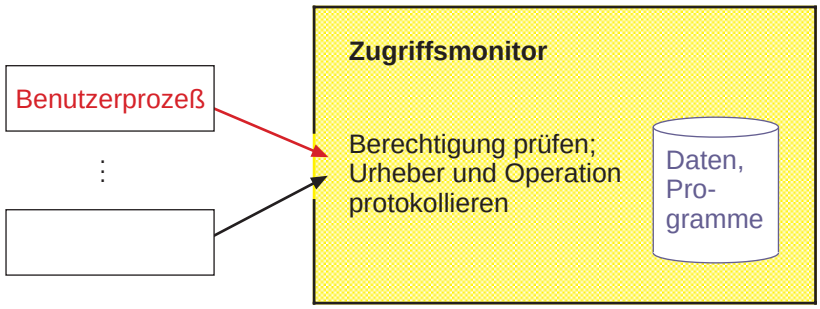

Abbildung 2. Gewährung von Rechten über einen Zugriffsmonitor

Beispiel: Rechte werden z.B. in einer Zugriffskontrollmatrix gespeichert. Typische Rechte sind Schreiben, Lesen, Verändern, Löschen, Ausführen.

Die Rechtevergabe selbst wird **Autorisierung** (*authorization*) genannt.

1.6 Protokollierung

Kein System ist hundertprozentig sicher, bei der Rechtevergabe können Fehler gemacht werden und regelwidriges Verhalten eines Mitarbeiters (gemäß den Organisationsrichtlinien eines Unternehmens) bedeutet nicht unmittelbar eine Verletzung der technischen Sicherheitsvorkehrungen.

Sollen im Nachhinein Angriffe und Fehlverhalten erkannt werden, müssen sicherheitsrelevante Vorgänge durch das System protokolliert werden. Ein späteres Verändern oder Vernichten der sog. Log-Dateien durch den Angreifer muß dabei ausgeschlossen sein.

Protokollierung muß in Einklang mit den datenschutzrechtlichen Bestimmungen stehen. Der Mißbrauch von Log-Dateien muß durch technische und organisatorische Maßnahmen verhindert werden.

Typische Protokolle enthalten Daten über alle Login-Versuche (erfolgreich, nicht erfolgreich), Logout, Ändern von Passwörtern, lesende und schreibende Zugriffe auf Dateien, Installation von Software.

Wenn die Auswertung protokollierter Vorgänge automatisch (oder sogar in nahezu Echtzeit) erfolgt, spricht man von **Intrusion-Detection**.

1.7 Sicherheit des Betriebssystems

Die Sicherheit des Betriebssystems ist essentiell für die sichere Benutzung von Anwendungen auf einem Rechner. Da alle Programmbefehle und Daten vom Betriebssystem interpretiert und verarbeitet werden, kann es keine Manipulationssicherheit oder Vertraulichkeit reiner Softwareanwendungen und ihrer Daten vor dem Betriebssystem geben (nach oben zeigender Pfeil in Abbildung 3).

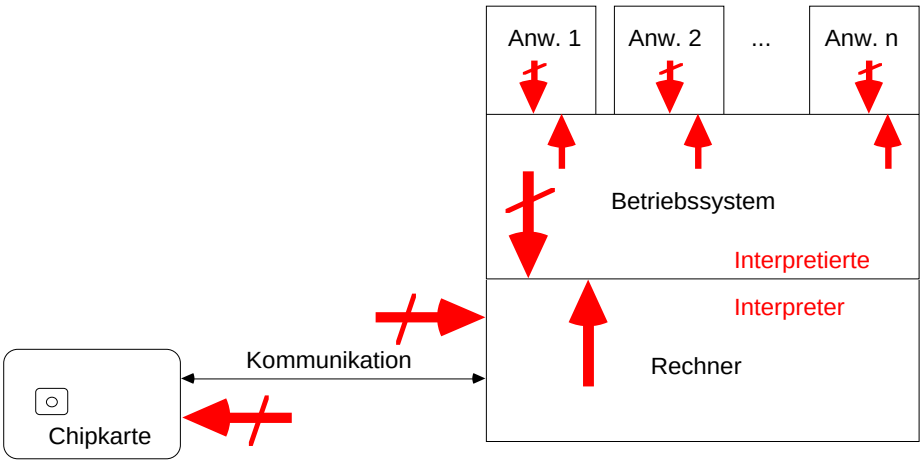

Abbildung 3. Verhältnis von Schichtenstruktur und Angriffserfolg

Umgekehrt ist ein sicheres Betriebssystem jedoch in der Lage, sich vor Angriffen durch Anwendungen oder – prinzipieller formuliert – durch höhere Schichten eines Systems zu schützen (durchgestrichene, nach unten zeigende Pfeile in Abbildung 3). Die Schichtenstruktur von Systemen macht auch klar, daß dies ebenso für die Beziehung zwischen Betriebssystem und Rechner gilt, auf dem das Betriebssystem läuft. Für den Fall, daß sichere Systemkomponenten lediglich kommunizieren, sind unkontrollierbare Zugriffe nicht möglich, da hier nichts gegenseitig ausgeführt oder interpretiert wird. Um Angriffe des zwischen den Systemkomponenten liegenden Mediums auszuschließen, kommen kryptographischen Verfahren (Verschlüsselung, Schutz vor Verfälschung, etc.) zum Einsatz.

Besonders kritisch wird die Situation, wenn die für seinen Benutzer vertrauenswürdigen Systemteile (Geräte) zum Erbringen ihrer Funktion in Systemteile (Geräte) anderer integriert (z. B. hineingesteckt) werden müssen. Ein besonders kritisches Gerät ist in dieser Beziehung die Chipkarte. Im Normalfall muß die Chipkarte, die durch eine Persönliche Identifikationsnummer (PIN) vor unberechtigter Verwendung geschützt ist, bei der Benutzung in ein Lesegerät eingeführt werden. Die Tastatur am Lesegerät ermöglicht die Eingabe der PIN und damit die Aktivierung der Chipkarte. Der Besitzer der Chipkarte darf in einem solchen Fall nicht nur seiner Chipkarte vertrauen, sondern muß seinen Vertrauensbereich auch auf das Lesegerät erweitern, da das Lesegerät in Kenntnis des Aktivierungscodes gelangt und somit in der Lage ist, nicht autorisierte Aktionen (z. B. Zahlungen, digitale Signaturen) auszulösen, zumindest solange die Chipkarte im Leser verbleibt oder wenn sie zu einem späteren Zeitpunkt erneut eingeführt wird.

1.8 Schutz vor Computerviren

In vielen heute verbreiteten PC-Betriebssystemen (DOS, Windows 95/98/ME/CE, MacOS) fehlt die Zugriffskontrolle. Dies begünstigt die Ausbreitung von Computerviren[8,9,10] und Trojanischen Pferden erheblich.

Ein **Computervirus** ist ausführbarer Code, der sich in fremde Programme einpflanzt, dort ausgeführt wird und ggf. eine sog. **Schadensfunktion** ausführt. Ein **Wurm** ist ein ausführbares Programm, das sich über Rechnernetze verbreitet und ggf. eine Schadensfunktion ausführt. Ein **Trojanisches Pferd** ist ein Rechnerprogramm, das neben einer bekannten (vom Anwender gewünschten) Funktion eine (nicht gewünschte) Schadensfunktion ausführt.

Viren, Würmer und Trojanische Pferde können nicht nur die Integrität und Verfügbarkeit von Daten und Programmen verletzen, sondern alle Schutzziele, also auch die Vertraulichkeit von Daten. Im schlimmsten Fall können Viren und Trojanische Pferde ihre Schadensfunktion modifizieren und sogar sich selbst zerstören, nachdem sie ihre „Aufgabe" erfüllt haben, um die hinterlassenen Spuren zu vernichten.

In IT-Systemen mit Zugriffskontrolle kann die Ausbreitung von Viren durch das **Prinzip der geringstmöglichen Privilegierung** (*principle of least privilege*) verhindert werden. Das bedeutet, jedes Programm bekommt nur die minimal notwendigen (Schreib-)Rechte.

Bei Würmern und Trojanischen Pferden kann der Schaden zumindest auf die autorisierten Ressourcen begrenzt werden. Die Beschränkung von Ausführungsrechten verhindert die Verbreitung von Würmern. So ist beispielsweise die Weiterverbreitung von E-Mail-Würmern durch die automatisierte Ausführung von in E-Mails eingebetteten ausführbaren Dateien sehr leicht möglich und führte zu großen Schäden.[11]

1.9 Schutz der Verfügbarkeit und Vermeidung von Fehlern

Um Vertrauenswürdigkeit zu erreichen, muß es möglich sein, Systeme zu validieren. Das bedeutet, unabhängige, (frei) wählbare Experten vergewissern sich von der korrekten Implementierung und Arbeitsweise eines Systems gemäß einer allgemein akzeptierten Spezifikation. Da dem normalen Anwender meist weder die Mittel noch das Wissen zur Verfügung stehen, um Systemkomponenten oder gar ganze Systeme zu validieren (geschweige denn zu verifizieren), kann diese Aufgabe durch **unabhängige Stellen** durchgeführt und das System so zertifiziert werden.

Im weiteren Sinn bedeutet Begrenzung von Fehlern auch, daß Systeme nicht nur von einem Hersteller (Entwickler, Administrator) entwickelt, produziert, angeboten und betreut werden sollen, sondern von vielen. Solange beispielsweise kein perfektes Betriebssystem existiert, sollte der Anwender die Auswahl unter mehreren Betriebssystemen haben.

Ein interessantes Konzept zur Vermeidung von Fehlern ist die Politik der Offenheit, insbesondere bei der Erstellung und Validierung von Software. **Open Source**[12] kann helfen, „Fehler" in Software schneller zu finden und die Qualität der Software durch Verfügbarkeit von allgemein nutzbaren Modulen zu verbessern. Im Sicherheitsbereich ist Offenheit ohnehin ein gutes Mittel zur Erhöhung der Vertrauenswürdigkeit. Kein Kundiger würde der Sicherheit eines Verschlüsselungsalgorithmus ernsthaft vertrauen, wenn dieser nicht öffentlich bekannt und durch Experten auf Sicherheitslücken geprüft worden ist.

---

[8] Peter J. Denning (ed.): Computers under attack: intruders, worms and viruses. ACM Press, New York 1990.

[9] David Ferbrache: A Pathology of Computer Viruses. Springer-Verlag, Berlin 1992.

[10] Winfried Gleißner, Rüdiger Grimm, Siegfried Herda, Hartmut Isselhorst: Manipulation in Rechnern und Netzen – Risiken, Bedrohungen, Gegenmaßnahmen. Addison-Wesley, Bonn 1989.

[11] vgl. Loveletter, http://www.sarc.com/avcenter/venc/data/vbs.loveletter.fw.a.html

[12] Kristian Köhntopp, Marit Köhntopp, Andreas Pfitzmann: Sicherheit durch Open Source? Chancen und Grenzen. Datenschutz und Datensicherung DuD 24/9 (2000), 508-513.

Diversität

Kryptographische Systeme allein können das Schutzziel Verfügbarkeit nicht realisieren. Die Verfügbarkeit von Daten, Programmen und Diensten kann jedoch durch die adäquate technische Gestaltung der Kommunikationsinfrastruktur sichergestellt werden. Dabei spielen der Grad an **Diversität** und **Entwurfskomplexität** eine entscheidende Rolle.

So sollte im Interesse der Durchschaubarkeit eine Kommunikationsinfrastruktur mit geringstmöglicher Entwurfskomplexität gewählt werden, damit sie keine, zumindest keine schweren, verborgenen Entwurfsfehler enthält.

Ein diversitäres Kommunikationsnetz mit mehrfach redundanter und unterschiedlicher Leitungsführung kann z.B. den Totalausfall bei Ausfall von Teilen des Netzes vermeiden. Bei Funknetzen könnte auf unterschiedliche Frequenzbänder ausgewichen werden, sobald Störungen auftreten. Besonders problematisch sind evtl. vorhandene Diversitätsengpässe, z.B. Netzübergänge.

Verfügbarkeit kann nicht isoliert von den Schutzzielen Vertraulichkeit und Integrität betrachtet werden. So könnte z.B. die Störung der Verfügbarkeit für andere Teilnehmer zur Deanonymisierung und damit Beobachtbarkeit eines bestimmten Teilnehmers führen, falls die Teilnehmer zusammen in einer Anonymitätsgruppe hätten handeln sollen. Andererseits können z.B. Authentikationsmaßnahmen den unerkennbaren und unentdeckbaren Betriebsmittelentzug (und damit Verfügbarkeitsverlust) für andere Teilnehmer verhinden, wenn jeder Zugriff auf Betriebsmittel nur authentisiert erfolgen darf.

Verfügbarkeit im Internet

Die in den letzten Jahren bekannteste Angriffsklasse auf Rechner im Internet sind Angriffe auf die Verfügbarkeit. Diese Angriffe werden auch als Denial-of-Service (DoS) bezeichnet.

DoS-Angriffe können

- entweder durchgeführt werden, indem der Angreifer versucht, in den Rechner einzudringen und sich die notwendigen Rechte verschafft, um einen Service zu beeinträchtigen,
- oder der Angreifer versucht, den Dienst mit Service Requests dermaßen zu überlasten, daß er für normale Anfragen nicht mehr verfügbar ist (Flooding).

Das unberechtigte Eindringen bzw. Nutzen von Diensten läßt sich durch geeignete Zugangskontrollmechanismen (siehe Abschnitt VI.1.4) verhindern. Das Flooding eines Dienstes mit Anfragen läßt sich dadurch jedoch nicht verhindern. Schließlich kann der Zugangskontrolldienst selbst durch Anfragen überlastet werden, die zwar sowieso abgelehnt würden. Aber die Berechtigungsprüfung kostet natürlich Betriebsmittel.

Bei öffentlichen und frei zugänglichen Dienstangeboten (z.B. im World Wide Web) erfolgt meist keine Zugangskontrolle. Diese Dienste werden meist durch Flooding angegriffen.

Ein Beispiel eines Angriffs durch Flooding ist die Smurf-Attack[13]. Dabei handelt es sich um eine distributed Denial-of-Service (dDoS) Attack. Der Angriff beruht auf dem Ping-Service, den nahezu jeder an das Internet angeschlossene Rechner anbietet. Um herauszufinden, ob ein Rechner im Internet erreichbar ist, sendet man ihm eine Ping-Anfrage. Die Ping-Anfrage enthält, wie jedes IP-Paket, die IP-Adresse des Absenders (Anfragers) und die IP-Adresse des Empfängers, also des Rechners, der die Ping-Anfrage erhalten soll. Nur bei Erreichbarkeit sendet der angefragte Rechner eine Antwort (Pong) an den Absender zurück.

Aufgrund eines schlecht konfigurierten lokalen Netzes kommt es vor, daß nicht nur der angefragte Rechner mit einem Pong anwortet, sondern gleich mehrere. Dies tritt dadurch auf, daß der eigentlich angefragte Rechner, der als Gateway zu einem lokalen Netz dient, die Ping-Anfrage fälschlicherweise an alle seine angeschlossenen lokalen Rechner weitergibt, die korrekt darauf antworten. Das Gateway sendet diese Antworten nun (ebenfalls fälschlicherweise) zurück an den Absender. Die Folge ist eine Vervielfachung der Pong-Nachrichten.

---

[13] Attack (CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attack

Ziele des Angriffs ist es, den angegriffenen Rechner mit ankommenden IP-Paketen so zu überfluten, daß er die ankommende Datenmenge nicht mehr verarbeiten kann und alle seine Dienste einstellt. Da hierfür eine gewaltige Menge an Datenpaketen versendet werden muß, sind mehrere Rechner nötig, die synchronisiert die Datenflut für das Opfer erzeugen.

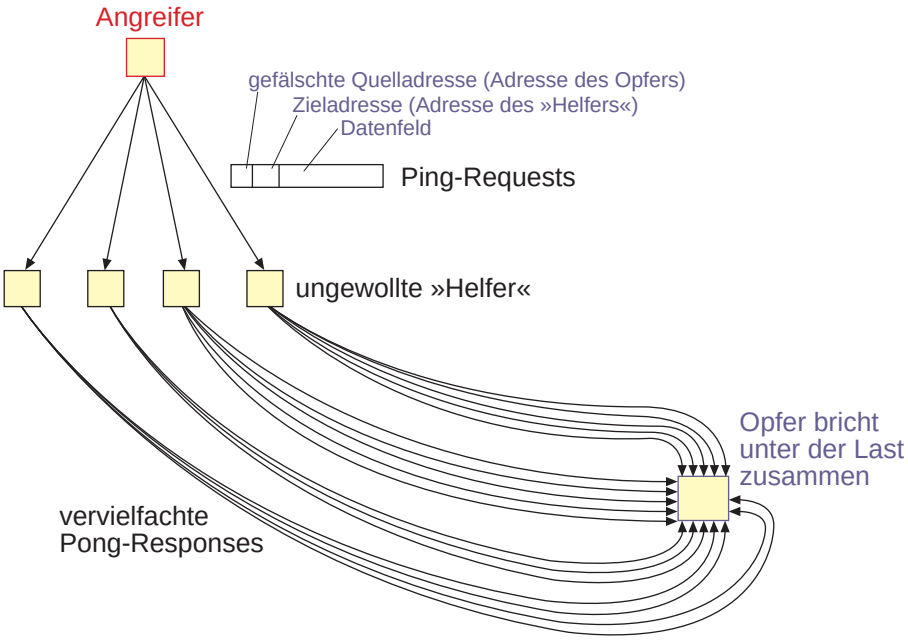

Abbildung 4. Distributed Denial-of-Service Attack

Der Angreifer sucht sich zunächst eine genügend große Anzahl schlecht administrierter Rechner (Abbildung 4), die mit einem Vielfachen an Pong-Nachrichten auf ein Ping antworten. Ein Eindringen in den Rechner ist wie beschrieben hierfür nicht nötig.

Der Angreifer sendet nun Ping-Anfragen mit gefälschter Absenderangabe (der IP-Adresse des Opfers) an diese Rechner. Da die Absenderadresse falsch ist, erhält das Opfer die Pong-Nachrichten und bricht unter der Menge der empfangenen Datenpakte zusammen.

Der eigentliche Angreifer bleibt unerkannt, da seine IP-Adresse in den Datenpaketen nirgends auftaucht.

1.10 Firewalls

Firewalls[14] dienen der Abschottung eines Intranets bzw. eines sicherheitsempfindlichen Teilnetzes vor unberechtigten Zugriffen von **außen**. Das zu schützende Netz hat als einzigen Zugangspunkt die Firewall: Alle Datenpakete zum und vom Intranet müssen die Firewall passieren.

Firewalls sind regelbasierte Filtersysteme. Die Filterfunktionen sind auf drei Ebenen der Kommunikationsprotokolle angesiedelt:

- **Paketfilter** überprüfen anhand der IP-Adresse des Absenders und Empfängers sowie der Portnummer (TCP oder UDP), ob das Datenpaket die Firewall passieren darf. Teilweise analysieren Paketfilter auch den Inhalt der Datenpakete.
- **Circuit Level Gateways** überprüfen TCP- oder UDP-Verbindungen, ob sie die Firewall passieren dürfen. Verbindungen setzen sich aus vielen Datenpaketen zusammen. Die Firewall ersetzt bei Verbindungen, die das Intranet verlassen, die ursprüngliche Absenderadresse durch die eigene IP-Adresse und verbirgt somit die interne Netzstruktur.

[14] Stefan Strobel: Firewalls für das Netz der Netze. dpunkt-Verlag, Heidelberg 1997.

- **Application Level Gateways**, auch **Proxies** genannt, implementieren die Schnittstelle des Clients als auch des Servers eines Dienstes.

Während Paketfilter und Circuit Level Gateways eingesetzt werden können, ohne daß der Anwender im Intranet davon etwas mitbekommen muß[15], müssen die Anwendungen den Gebrauch von Proxies unterstützen. Dies ist heute bei nahezu allen relevanten Anwendungen (Browser, Filetransfer, News, Napster) der Fall. Da für jede Anwendung (bzw. deren Protokoll) ein eigener Proxy vorhanden sein muß, können nicht ohne weiteres neue Anwendungen proxy-tauglich gemacht werden. Abhilfe schafft hier ein sog. SOCKS-Proxy, der eine universelle Proxy-Schnittstelle bereitstellt.

Grenzen von Firewalls

Firewalls sind eine „best-practice"-Technik, d.h. sie stellen einen **Kompromiß zwischen Schutz und Kosten** dar. Besser aber teurer wäre es, jeden einzelnen Rechner im Intranet mit entsprechenden Filterfunktionen auszustatten. Firewalls haben klare Grenzen bzgl. des erreichbaren Schutzes:

- Sie schützen erstens nicht vor Angriffen von innen. Wenn ein Mitarbeiter beispielsweise einen illegalen Modemzugang im sicherheitsempfindlichen Teilnetz installiert, werden die Daten an der Firewall vorbei geschleust.
- Zweitens müssen die Filterfunktionen naturgemäß so konfiguriert sein, daß vernünftiges Arbeiten noch möglich ist. Dies führt in der Praxis jedoch zu einem schrittweisen „Aufweichen" der Firewall-Funktion.
- Drittens schützen selbst sehr restriktive Filterfunktionen nicht vor unerlaubtem oder gar unbemerktem Datenfluß: Mit Techniken wie HTTP-Tunneling ist es möglich, verdeckte Kanäle zu realisieren: In harmlos erscheinenden Daten (hier: Anfrage an einen Webserver) können andere Daten unbemerkt transportiert werden. Hierzu muß sich ein Benutzer lediglich ein harmlos erscheinendes, ihm nutzbringendes Programm „eingefangen" haben, das in Wirklichkeit ein Trojanisches Pferd ist.
- Viertens schützt eine Firewall auch nicht vor Trojanischen Pferden. Die Aktivierung eines Virenscanners auf der Firewall dagegen ist möglich und nutzbringend, solange die Nachrichteninhalte nicht ende-zu-ende-verschlüsselt sind.

Firewall-Architekturen

Firewalls sollen Angriffe von außen verhindern, konkreter, sie sollen das Eindringen in das sicherheitsempfindliche Intranet verhindern. Da es selbst bei sorgsamer Administration der Firewall und des Netzes vorkommen kann, daß ein Eindringversuch erfolgreich ist, werden Firewalls in unterschiedlich aufwendigen Architekturen betrieben.

Die **sicherste Form** eines Firewalls ist eine Kombination aus internem und externem Paketfilter mit dazwischen liegendem Gateway (sog. Bastion-Host), siehe auch Abbildung 5.

[15] Informatiker sagen: Paketfilter und Circuit Level Gateways sind für die Anwendung transparent.

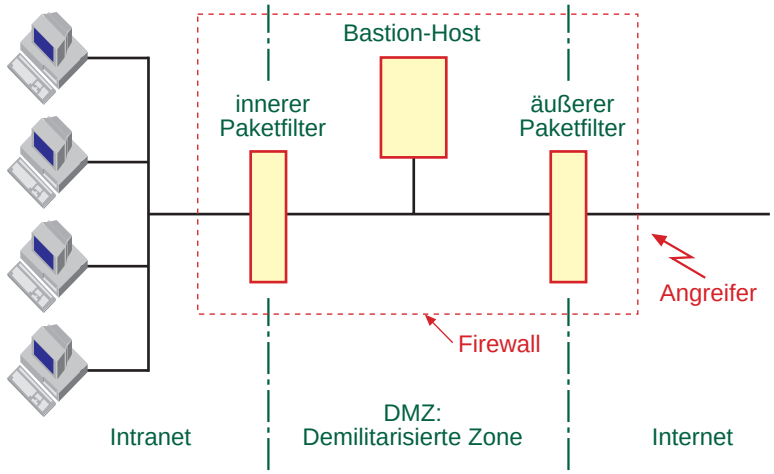

Abbildung 5. Schutz eines Intranets durch Firewall

Das Segment zwischen den **beiden Paketfiltern** wird klangvoll „demilitarisierte Zone“ (DMZ) genannt. Die Paketfilter erlauben jeweils nur die Kommunikation mit dem Bastion-Host, so daß ein Eindringling, der den äußeren Paketfilter überwunden hat, zwar den Bastion angreifen kann, aber keinen Rechner des Intranets. Erst wenn der Bastion-Host und der innere Paketfilter überwunden sind, hat der Angreifer auch Zugang zum Intranet.

Schwächere Firewall-Architekturen verzichten zu Lasten der Sicherheit und zugunsten der geringeren Kosten auf den inneren Paketfilter, manche sogar auf den äußeren Paketfilter.

1.11 Sicherheitsmanagement

Je mehr Funktionen eine Organisation mit Hilfe von IT-Systemen erledigt, umso abhängiger wird sie von der fehlerfreien und verläßlichen Funktion der Systeme. Im Rahmen des Sicherheitsmanagements sind folglich entsprechende Maßnahmen zu treffen:

1. Entwicklung einer IT-Sicherheitspolitik und eines IT-Sicherheitskonzeptes,
2. Realisierung der IT-Sicherheitsmaßnahmen,
3. Schulung und Sensibilisierung der Benutzer,
4. Erhaltung der IT-Sicherheit im laufenden Betrieb.

Im Rahmen des IT-Sicherheitskonzeptes werden Maßnahmen festgelegt, die auf weite Teile der Organisation Einfluß haben. Hierzu zählen:

- **Infrastruktur:** Physische Zugangs- und Zutrittskontrolle, Stromversorgung, Feuerschutz, Klimatisierung;
- **Organisation:** Überwachung, Kontrolle, Dokumentation, permanente Anpassung des Sicherheitskonzeptes an veränderte Gegebenheiten;
- **Personal:** Maßnahmen bei Auswahl, Einstellung, Ausscheiden; fortlaufende Schulung;
- **Hardware und Software:** Hardware-, Betriebssystem- und Softwareauswahl, Passwort- und Virenschutz;
- **Kommunikation:** Netztopologie, Netzverwaltung, -administration, Übertragungssicherung, Protokollierung von Zugriffen;
- **Notfallvorsorge:** Datensicherungskonzept (Backup), Versicherungen, Notfallrechenzentrum.

Konkrete Maßnahmen- und Gefährdungskataloge sowie Informationen zum IT-Grundschutz findet man z.B. im Grunschutzhandbuch[16] des Bundesamtes für die Sicherheit in der Informationstechnik (BSI).

[16] http://www.bsi.de/gshb/