Bedrohungen im Netz

In diesem Kapitel werden die potentiellen Bedrohungen beschrieben, die in Netzen wie Intranets und dem Internet bestehen.

Angreifer

Personen greifen Rechnersysteme und Netzwerke an. Sie tun dies aus sehr unterschiedlichen Motiven.

Im Folgenden werden einige Arten von Angreifern und deren Ziele dargestellt:

- Hacker
  Hacker brechen in Rechnersysteme und Netzwerke ein, weil sie darin eine Herausforderung sehen und mit dem Erfolg ihren Status vergrößern wollen. Oft handelt es sich um Jugendliche, die aus »Spieltrieb«, also ohne böse Absicht handeln. Sie sind aber unberechenbar und können hohen Schaden verursachen.
- IT-Spione
  Bezahlte Spezialisten – teilweise mit einem sehr hohem Budget – versuchen, über gezielte Angriffe an Informationen zu kommen. Ihre Ziele sind politisch oder auch wirtschaftlich begründet (siehe »Echelon«).
- IT-Terroristen
  Terroristen können Rechnersysteme und Netzwerke angreifen, um aus politischen Gründen Angst und Chaos zu verursachen.
- Unternehmens-Cracker
  Dies sind Mitarbeiter, die auf Rechnersysteme und Netzwerke von Konkurrenzunternehmen zugreifen, um ihrem Unternehmen finanzielle Vorteile zu schaffen. Dazu spähen sie beispielsweise Entwicklungsunterlagen oder Strategiepläne aus.
- Professionelle Kriminelle
  Diese Personen wollen sich mit Angriffen persönlich bereichern, beispielsweise durch die nicht bezahlte Nutzung von Dienstleitungen oder durch das Abbuchen von fremden Konten.
- Vandalen
  Vandalen sind Personen, die Angriffe durchführen, um Organisationen oder Personen gezielt Schaden zuzufügen.

3.1 Angriffsmöglichkeiten in Kommunikations-Systemen

Die stärksten Bedrohungen von IT-Systemen zielen auf das Kommunikations-System, das heißt auf die Nachrichten, die über Systeme wie Internet und Intranet ausgetauscht werden. Zunächst werden die verschiedenen Angriffsarten definiert und anschließend die Schäden kategorisiert, die durch Angriffe entstehen können.

Auf eine Nachricht (ein oder mehrere IP-Pakete) reagiert ein Empfänger mit einem bestimmten Verhalten (Abb. 3.1):

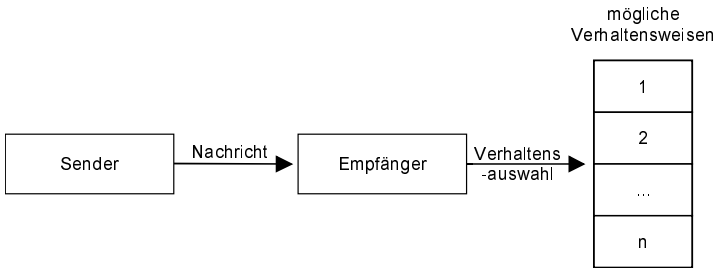

Abb. 3.1: Reaktionsmöglichkeiten des Empfängers einer Nachricht

Ein Angreifer, der die Kommunikationsverbindung abhört, kann das Verhalten des Empfängers und des Senders interpretieren. Der Angreifer kann die Reaktionen des Empfängers zielgerichtet beeinflussen, wenn er die Möglichkeit hat, die Nachricht zu wiederholen, zu verändern, zu löschen oder zu ergänzen.

Aus dieser Überlegung heraus werden grundsätzlich zwei Arten von Angriffen unterschieden: passive Angriffe und aktive Angriffe.

3.1.1 Passive Angriffe

Bei passiven Angriffen werden die übertragenen Nachrichten und der Betrieb des Kommunikations-Systems nicht geändert. Passive Angriffe sind Bedrohungen, die vom Angreifer bewusst und gezielt durchgeführt werden, um sich unerlaubt Informationen zu beschaffen.

Passive Angriffe können zum Beispiel mit Hilfe von Klemmen oder Induktionsschleifen an der Leitung oder durch das Abfangen der Signale von Richtfunk- und Satellitenverbindungen durchgeführt werden (Abb. 3.2).

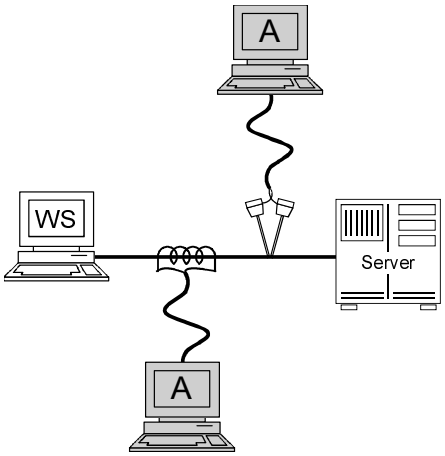

Abb. 3.2: Passive Angriffe auf Nachrichten oder auf das Kommunikations-System

Man kann folgende passive Angriffsarten unterscheiden:

- Abhören von Daten
  Ein Abhörer gelangt unmittelbar in den Besitz der Nachricht und kann sie zu seinem Zweck verwerten. Beispielsweise kann ein Angreifer bei einer IP-Verbindung zwischen einem Telnet-Server und einem Telnet-Client während der Login-Prozedur die Identität und das Passwort eines Teilnehmers abhören und später mit diesem Passwort unerlaubt Zutritt zum Serversystem erlangen. Weitere Möglichkeiten sind das Abfangen von vertraulichen Informationen, wie Entwicklungsunterlagen von neuen Produkten, das Abhören von Daten, die unter das Datenschutzgesetz fallen, oder Angebote auf Ausschreibungen. Solche Angriffe sind bei der Nutzung von frei zugänglichen LAN-Anschlüssen problemlos durchführbar.
- Abhören der Teilnehmer-Identitäten
  Der Lauscher erfährt, welche Teilnehmer (Benutzer oder Rechnersysteme) untereinander eine Datenverbindung aufbauen und Daten austauschen. Allein aus der Kenntnis, wer mit wem zu welchem Zeitpunkt Nachrichten ausgetauscht hat, sind oft Rückschlüsse auf den Inhalt der Nachricht oder auf das Verhalten der Teilnehmer möglich. Wenn zum Beispiel jemand auf die Web-Seiten eines Waschmaschinenherstellers zugreift, kann vermutet werden, dass er eine Waschmaschine kaufen möchte. Tauschen zwei bis dahin konkurrierende Unternehmen in großem Umfang Nachrichten aus, kann dies ein Anzeichen für eine bevorstehende Zusammenarbeit sein.

- Verkehrsflussanalyse
  Auch wenn die Daten verschlüsselt sind, ist es einem Abhörer möglich, durch eine »Verkehrsflussanalyse« gewisse Informationen zu erhalten. Dabei kann es sich um Größenordnungen, Zeitpunkte, Häufigkeit und Richtung des Datentransfers handeln. Diese Informationen können für bestimmte spezielle Anwendungen interessant sein, wie etwa Börsen-Transaktionen oder militärische Operationen.

Spezielle Gefahren beim Einsatz lokaler Netze

Besonderen passiven Angriffen sind lokale Netze (LANs) ausgesetzt, da sie im Allgemeinen »Broadcast-Medien« verwenden. Es werden alle Nachrichten an alle Teilnehmer gesendet und es wird davon ausgegangen, dass die Teilnehmer nur die Nachrichten verwenden, die für sie bestimmt sind. In der Praxis werden zusätzliche Netzwerk-Steckdosen eingerichtet, um flexibel für Umzüge, weitere Rechnersysteme etc. zu sein. Diese zusätzlichen Steckdosen sind meist nicht blockiert, solange sie nicht benutzt werden. Sie können dadurch jederzeit missbraucht werden, um Analysegeräte anzuschließen und den gesamten Nachrichtenstrom mitzuverfolgen.

Lokale Netze sind aber auch so konzipiert, dass im laufenden Betrieb zusätzliche Steckdosen und Rechnersysteme montiert werden können, ohne den Verkehr zu stören. Diese Flexibilität und Robustheit ist aus Sicht der Datensicherheit von großem Nachteil. Beide beschriebenen Faktoren bergen die Gefahr, dass zusätzliche Rechnersysteme unbefugt und unbemerkt angeschlossen werden können. Aber auch die Stationen befugter Teilnehmer können dazu verwendet werden, den gesamten Nachrichtenstrom abzuhören.

Mit einfachen Hilfsmitteln wie Protokollanalysatoren (z. B. TCPDump oder Snoop als Standard-UNIX-Tools) können möglicherweise von jedem Rechnersystem im LAN alle Pakete mitgelesen werden. Da viele Organisationen die Systemadministration der Rechnersysteme »remote« durchführen, können »root«-Passworte mitgelesen werden. Mit deren Hilfe können dann weitere Angriffe durchgeführt werden.

Protokollmitschnitt einer Telnet-Session

Im folgenden Protokollmitschnitt einer Telnet-Sitzung ist die Phase des Login festgehalten. Die Software, die den Protokollmitschnitt realisiert hat, kann auf jedem üblichen PC laufen, der an ein LAN angeschlossen ist (siehe Abb. 3.3). An das Rechnersystem, mit dem der Mitschnitt durchgeführt wurde, werden von der Analysesoftware (A) keine besonderen Anforderungen gestellt.

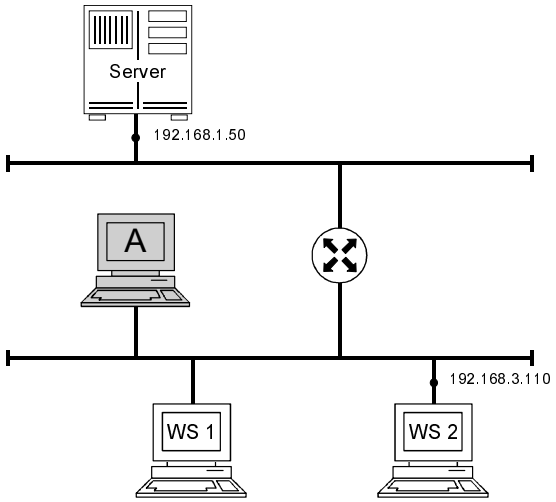

Abb. 3.3: Passiver Angriff mit Hilfe eines Protokollanalysators

Der Benutzer der Workstation 2 hat ein Login am Server durchgeführt. Als Benutzeridentifikation wurde »Nutzer1« eingegeben. Diese Eingabe wurde vom Server zur Kontrolle zurückgesendet, aus diesem Grund sind die einzelnen Buchstaben doppelt im Protokollmitschnitt zu sehen. Das Passwort, das der Benutzer »Nutzer 1« verwendet hat, lautet »1beutlin« (siehe Tab. 3.1). Die Buchstaben des Passworts werden vom Server nicht zurückgesendet, so dass sie nur einmal zu sehen sind. Diese Eigenschaft erleichtert die Suche nach dem Passwort in Protokollmitschnitten.

Wenn ein Protokollmitschnitt aufgenommen wird, während sich alle Netzwerk-Teilnehmer am Server einloggen – beispielsweise bei Arbeitsbeginn in einem Unternehmen –, können alle Passworte festgehalten werden.

Es muss betont werden, dass mangelhafte Vertraulichkeit ein großes Problem beim Betrieb lokaler Netze ist, da sie auch mit der mangelhaften Sicherheit der üblichen Zugangs- und Zugriffskontrollen auf Serversystemen und jeglichen Betriebsmitteln im lokalen Netz zusammenhängt.

Weitere Gefahrenpunkte in lokalen Netzen, an denen Nachrichten abgehört werden können, sind Hubs, Brücken, Router und Gateways.

Ziel	Quelle	Nachricht
192.168.3.110	192.168.1.50	Telnet :login:
192.168.1.50	192.168.3.110	Telnet :n
192.168.3.110	192.168.1.50	Telnet :n
192.168.1.50	192.168.3.110	Telnet :u
192.168.3.110	192.168.1.50	Telnet :u
192.168.1.50	192.168.3.110	Telnet :t
192.168.3.110	192.168.1.50	Telnet :t
192.168.1.50	192.168.3.110	Telnet :z
192.168.3.110	192.168.1.50	Telnet :z
192.168.1.50	192.168.3.110	Telnet :e
192.168.3.110	192.168.1.50	Telnet :e
192.168.1.50	192.168.3.110	Telnet :r
192.168.3.110	192.168.1.50	Telnet :r
192.168.1.50	192.168.3.110	Telnet :1
192.168.3.110	192.168.1.50	Telnet :1
192.168.1.50	192.168.3.110	Telnet :.
192.168.3.110	192.168.1.50	Telnet :..
192.168.3.110	192.168.1.50	Telnet :Password:
192.168.1.50	192.168.3.110	Telnet :1
192.168.1.50	192.168.3.110	Telnet :b
192.168.1.50	192.168.3.110	Telnet :e
192.168.1.50	192.168.3.110	Telnet :u
192.168.1.50	192.168.3.110	Telnet :t
192.168.1.50	192.168.3.110	Telnet :l
192.168.1.50	192.168.3.110	Telnet :i
192.168.1.50	192.168.3.110	Telnet :n
192.168.1.50	192.168.3.110	Telnet :.
192.168.3.110	192.168.1.50	Telnet :..
192.168.3.110	192.168.1.50	Telnet :Last login: Tue Apr 29 14:05:20 from merry..

Tabelle 3.1: Mitschnitt einer Telnet-Sitzung

Aktive Angriffe

Neben der Gefahr, abgehört zu werden, besteht das Risiko aktiver Angriffe, die den Nachrichtenstrom und/oder den Betrieb der Kommunikation verfälschen. Aktive Angriffe werden beispielsweise durch Auftrennen der Übertragungsleitungen oder mit Hilfe der Emulation von Übertragungsprotokollen durchgeführt (Abb. 3.4).

Bei aktiven Angriffen wird grob unterschieden zwischen Bedrohungen durch Dritte und Bedrohungen durch den Kommunikationspartner.

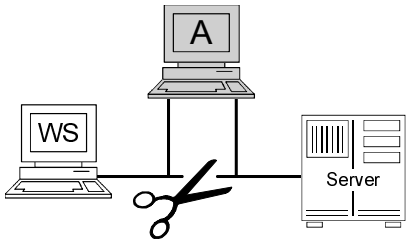

Abb. 3.4: Aktive Angriffe

Bedrohungen durch Dritte sind zum Beispiel:

- Wiederholen oder Verzögern von Informationen
  Durch Wiederholen oder Verzögern von Informationen kann der Empfänger irritiert oder zu einer falschen Aktion veranlasst werden.
  Beispiel: Mehrfache Überweisung eines Geldbetrags oder Wiederholung eines abgefangenen Logins.

- Einfügen oder Löschen bestimmter Daten
  Um ein System zu manipulieren, fügt ein Angreifer bestimmte Nachrichten oder Daten innerhalb der Nachrichten ein oder löscht sie. Ein Empfänger kann durch Unterdrückung oder zusätzlichen Empfang entscheidender Informationen zu einem falschen Verhalten veranlasst werden.
  Beispiel: In der E-Mail »Kaufen Sie *keinesfalls* neue Aktien« wird das Wort »*keinesfalls*« während der Übertragung gelöscht, so dass der Empfänger die Instruktion »Kaufen Sie neue Aktien« erhält.

- Modifikation von Daten
  Modifikation von Daten bedeutet, dass die Veränderung der Daten von den Kommunikationspartnern nicht erkannt wird. Durch Ändern der Daten während der Datenübertragung ist es dem Angreifer möglich, falsche Aktionen zu veranlassen /PoRi95/.

  Beispiel: Die Veränderung einer Kontonummer bei einer Geldüberweisung führt dazu, dass ein anderer als der intendierte Empfänger das Geld bekommt.

- Boykott des Kommunikations-Systems (Denial of Service)
  Wenn der Umfang von eingefügten oder unterdrückten Daten zu groß wird oder echtzeitorientierte Daten zu lange verzögert werden, kann hierdurch das gesamte Kommunikations-System boykottiert werden.

  Beispiel: Durch permanenten Verbindungsaufbau zu einem bestimmten Server kann dieser blockiert und isoliert werden.

Bedrohungen durch den Kommunikationspartner sind zum Beispiel:

- Vortäuschung einer falschen Identität (Maskerade-Angriff)
  Wenn sich ein Teilnehmer für einen anderen ausgibt, kann er sich Informationen erschleichen, die für diesen anderen Teilnehmer bestimmt waren, oder Aktionen auslösen, die nur der andere Teilnehmer veranlassen darf.

  Beispiel: Ein Teilnehmer verschafft sich unerlaubt Zugang zur einer Datenbank.

- Leugnen einer Kommunikationsbeziehung
  Der steigende Einsatz von Datenkommunikation zur Abwicklung vertraglich relevanter Vorgänge erfordert, dass sowohl der Abender einer Nachricht nicht leugnen kann, der Abender zu sein, als auch der Empfänger nicht abstreiten kann, die Nachricht erhalten zu haben.

  Beispiele: Die Bestellung von Waren bei einem Internet-Versandhändler oder der Abschluss von Verträgen über das Internet.

Trittbrettfahrer (Man in the middle)

Sogenannte Trittbrettfahrer verbinden sich zum Beispiel mit einem Knotenpunkt (Router oder Rechnersystem) im Internet und verfolgen einen Verbindungsaufbau mit. Die Verbindung wird dann nach der Authentikation des Benutzers für eigene Zwecke genutzt. Mit dieser Methode können Rechnersysteme, auf die der Zugriff eigentlich beschränkt ist, manipuliert und Authentikationsprozesse (auch kryptographische Methoden) unterlaufen werden.

Beschreibung eines Angriffs

Der Benutzer der Workstation 1 möchte einen Dienst des Servers X im Internet nutzen. Dazu baut der Benutzer eine Verbindung zum Server X auf und führt dort den notwendigen Login-Vorgang (Identifikation und Authentikation) durch.

Ein Angreifer (Rechnersystem A), der sich aktiv in die Kommunikationsverbindung im Internet eingeklinkt hat, verfolgt diese Prozedur und wartet, bis der Server die Bestätigung des erfolgreichen Login sendet. Diese Bestätigung gibt er nicht an die Workstation 1 weiter, sondern signalisiert dieser beispielsweise einen Verbindungsabbau. Der Angreifer trennt damit die Workstation 1 ab, ohne dass deren Benutzer den Angriff »bemerkt«. Nun kann der Angreifer die authentisierte Verbindung für sich und seine Ziele nutzen (Abb. 3.5). Diese Angriffsmethode kann auch bei kryptographischen Authentikationsverfahren benutzt werden.

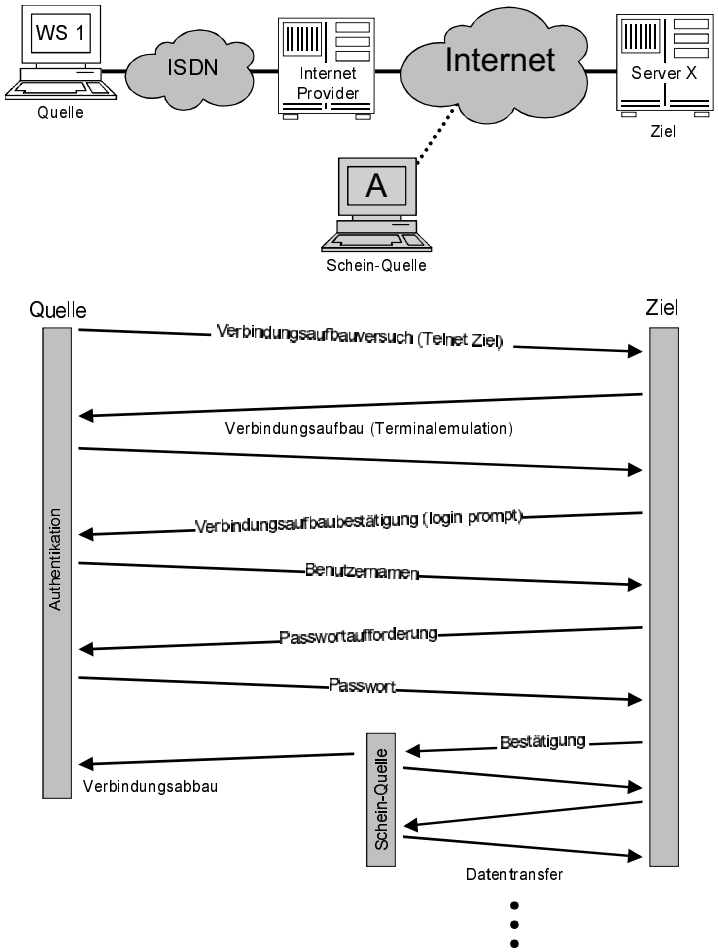

Abb. 3.5: Trittbrettfahrer

3.1.2 Zufällige Verfälschungsmöglichkeiten

Neben den Gefahren, die Kommunikations-Systemen durch absichtliche passive und aktive Angriffe drohen, gibt es auch verschiedene Möglichkeiten unbeabsichtigter Verfälschungen.

Unbeabsichtigte Verfälschungsmöglichkeiten sind zum Beispiel:

- Fehlrouting von Informationen
  In den Routern im Internet/Intranet können Informationen auf einen falschen Weg geraten und an einen fremden Teilnehmer ausgeliefert werden. Ein solches Fehlrouting kann bereits beim Verbindungsaufbau erfolgen, so dass die Verbindung zu einem falschen Teilnehmer hergestellt wird.

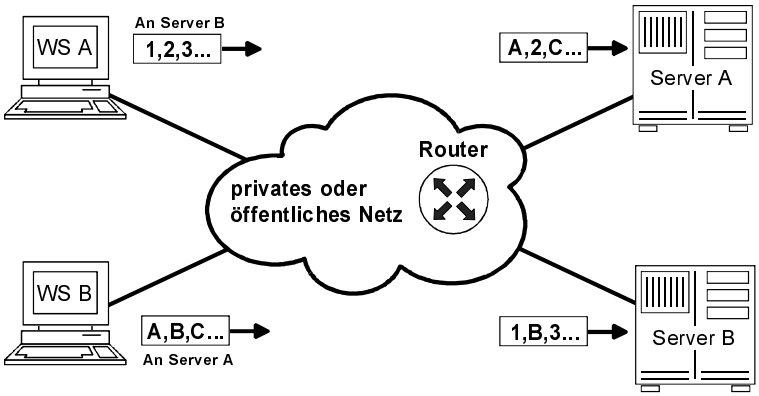

Abb. 3.6: Fehlrouting von Informationen

- Übertragungsfehler
  Übertragungsfehler können durch Übersprechen von Nachbarkanälen oder durch Wählgeräusche verursacht werden. Die Bitfehlerwahrscheinlichkeiten bei Datenübertragungswegen liegen zwischen 10^{-4} bis 10^{-7}. Auch hier können sicherheitskritische Fehler bei der Kommunikation über TCP/IP-basierte Netze auftreten.

- Software-Fehler
  99 % aller Software ist nicht verifiziert. Das bedeutet, dass in allen Softwarepaketen Fehler vorhanden sind, die in bestimmten Situationen zu Fehlreaktionen führen können.

  Beispiel: Die Software wählt durch einen internen Fehler einen falschen Teilnehmer an und sendet diesem vertrauliche Daten.

- Hardwarefehler durch Umwelteinflüsse
  Umwelteinflüsse wie elektromagnetische Emissionen können mit einem bestimmten Wahrscheinlichkeitsgrad die Ursache dafür sein, dass in einem Rechnersystem Bits umkippen, wodurch ein falsches Verhalten zu erwarten ist.

  Beispiel: Durch das Umkippen eines Bits im Router wird ein vertrauliches IP-Paket auf einem falschen logischen Kanal zu einem falschen Teilnehmer gesendet.

- Fehlbedienung
  Der Benutzer löst versehentlich Aktionen aus, die er nicht auslösen wollte.

  Beispiel: Der Benutzer wählt aus Versehen einen falschen Teilnehmer an und sendet diesem vertrauliche Informationen.

Fazit: Zufällige Verfälschungsmöglichkeiten können – wie aktive Angriffe – praktisch nicht ausgeschlossen werden. Wenn sie aber bekannt sind und beim Aufbau

der Kommunikations-Systeme berücksichtigt werden, kann der mögliche Schaden begrenzt werden.

3.2 Weitere Aspekte potentieller Bedrohungen bei Internet-Kommunikation

Fernmeldegeheimnis

In Deutschland gilt für alle Anbieter von Telekommunikationsdienstleistungen das Fernmeldegeheimnis. Dies bedeutet, dass Anbieter von Telekommunikationsdienstleistungen darlegen müssen, wie ihre Kommunikations-Systeme (Knoten, Netzwerkmanagement, usw.) abgesichert werden, um eine Manipulation von außen zu verhindern. Daher kann davon ausgegangen werden, dass im Fall einer Kommunikation über Netze in Deutschland und in anderen europäischen Ländern von den Telekommunikations-Dienstleistern ein hohes Maß an Sicherheit gewährleistet wird.

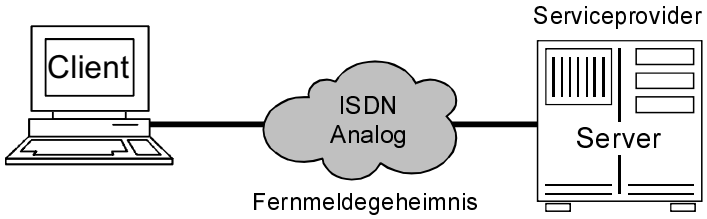

Abb. 3.7: Fernmeldegeheimnis

Beim Anschluss an das Internet, in dem die Kommunikation über Provider möglicherweise »um die ganze Welt geht«, verlassen wir diesen geschützten Bereich, da in anderen Ländern Vorschriften bezüglich des Fernmeldegeheimnisses nicht oder in nicht ausreichender Form existieren. Es kann also nicht davon ausgegangen werden, dass außerhalb Deutschlands oder Europas der gleiche rechtliche und technische Schutz gewährleistet ist.

Kommunikationswege der IP-Pakete im Internet

Da beispielsweise E-Mails unter Umständen über viele Netzknoten geleitet werden, worauf die Benutzer keinen Einfluss haben, ist die Gefahr eines organisierten Angriffs nicht zu unterschätzen.

Die Abbildung 3.9 zeigt, welchen abenteuerlichen Weg die IP-Pakete einer E-Mail genommen haben, die von der Niederlassung Aachen der Utimaco Safeware AG zu einem Institut der Rheinisch-Westfälischen Technischen Hochschule Aachen (RWTH Aachen) gesendet wurde, das nur 3 Kilometer entfernt liegt.

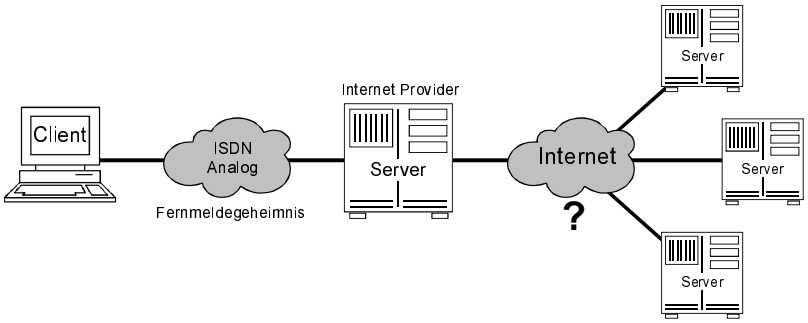

Abb. 3.8: Internet und das Fernmeldegeheimnis

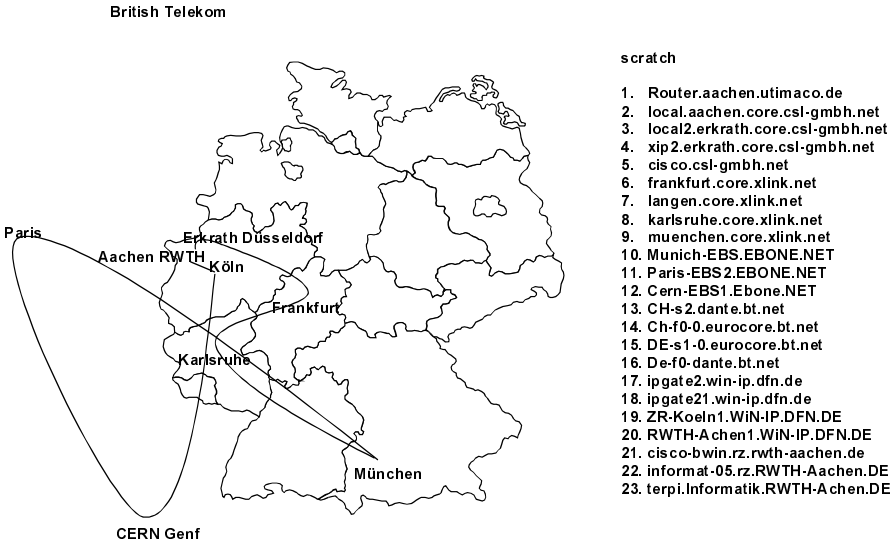

Abb. 3.9: Weg der IP-Pakete einer E-Mail

Diese E-Mail ist über 23 Router gelaufen, die sie empfangen und weitergesendet haben. Hierbei handelt es sich um ein harmloses Beispiel. Abhängig vom jeweiligen Internet-Provider werden manche IP-Pakete sogar über die USA geroutet.

3.2.1 Angriffstools aus dem Internet

Im Internet sind eine Reihe von Tools (z. B. ISS, Nessus) abrufbar, mit denen eine Analyse der Netzschwachstellen von TCP/IP-basierten Systemen, aber auch gezielte Angriffe möglich sind. Mit Hilfe dieser Tools kann jeder Benutzer, auch wenn er nicht über spezielles Fachwissen verfügt, solche Angriffe durchführen.

3.2.2 Implementierungsfehler in Anwendungen und fehlerhafte Konfigurationen

Anwendungen wie »Sendmail« wiesen in der Vergangenheit Implementierungsfehler auf, die es ermöglichten, auf einem entfernten IT-System beliebige privilegierte Kommandos auszuführen. Mit Hilfe dieser privilegierten Kommandos wurden dann Angriffe durchgeführt.

Für jeden Dienst, der über einen Netzzugang ermöglicht werden soll, existiert ein Daemon-Prozess, der falsch konfiguriert oder fehlerhaft sein kann, wodurch wiederum Angriffe durchgeführt werden können /CERT95/.

3.2.3 Echelon

Das größte Spionage-System der Welt heißt Echelon. Mit Hilfe von mehr als 120 Abhör-Satelliten werden über 3.000.000 Kommunikationsverbindungen (Telefon, Fax, ISDN, ...) in der Stunde analysiert. Es werden bis zu 90 % des Kommunikationsaufkommens im Internet gefiltert. Die US-amerikanische National Security Agency (NSA) beschäftigt zu diesem Zweck 140.000 Mitarbeiter, davon 20.000 bis 30.000 Mathematiker, und ist damit der weltweit größte Arbeitgeber für Mathematiker. Mit einem Budget von mehr als 10 Milliarden US-$ – sechsmal so viel wie das Budget des CIA – kann die NSA der militärischen und wirtschaftlichen Spionage »erfolgreich« nachgehen.

Kennen Sie Bad Aibling?

Bad Aibling ist das älteste Moorbad Bayerns, 50 Kilometer südöstlich von München im Mangfalltal gelegen, ein hübscher Kurort mit 16.000 Einwohnern. Er bietet einen schönen Ausblick auf die Tölzer Berge und über das Inntal (`www.kur-online.de`).

Gleichzeitig ist Bad Aibling der Standort eines US-Luftwaffengeländes mit einer Abhörstation. Unter der Leitung der NSA wird hier jede Art von Kommunikation abgehört und decodiert, die für die Sicherheit der USA von Interesse sein könnte.

Neben dem kaum vorstellbaren organisierten Abhören nimmt die NSA immer wieder (auf politischem oder finanziellem Weg – die Mittel dafür sind vorhanden) Einfluss auf Unternehmen, damit diese in ihre Sicherheitsprodukte sogenannte Trap-Doors oder andere verborgene Möglichkeiten einbauen. Diese Praxis ist durch viele Beispiele in der Vergangenheit belegt worden (Crypto AG, Lotus Notes, Microsoft, usw.).

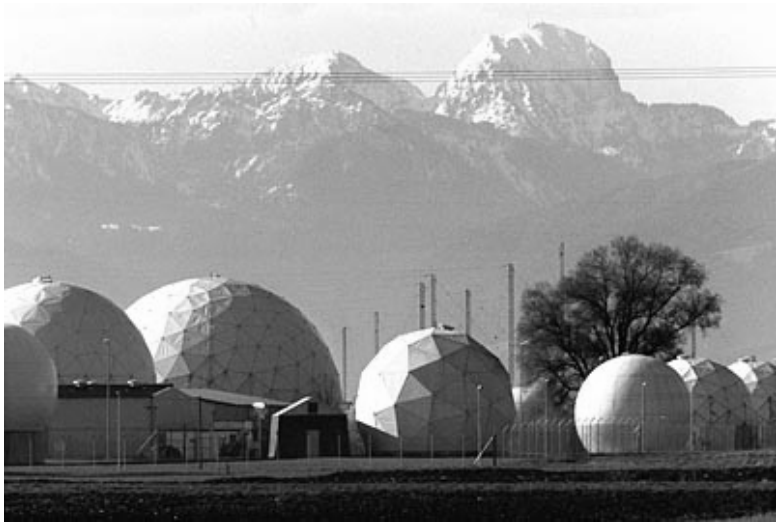

Abb. 3.10: Abhörstation der NSA in Bad Aibling

3.3 Wie hoch ist das Risiko?

Bei der Betrachtung der oben dargestellten potentiellen Bedrohungen stellt sich die Frage, wie groß die Eintrittswahrscheinlichkeit von Angriffen ist. Bei der Einschätzung des Angriffsrisikos spielen drei Faktoren eine wesentliche Rolle: Die lokalen Gegebenheiten, der Wert beziehungsweise die Verwertbarkeit der Daten und die Frage, wie hoch technischer und materieller Aufwand für einen Angreifer sind.

In Bürogebäuden mit mehreren Firmen verlaufen die Datenleitungen oft durch die Räumlichkeiten anderer Firmen oder sind im Hausanschluss-Raum für jedermann zugänglich. In diesem Fall ist es kein Problem, eine geeignete Stelle zu finden, an der die Datenleitungen angezapft werden können (Abb. 3.10).

Mögliche Angriffspunkte liegen auf den Fluren, in Kabelschächten, in der Tiefgarage und an den Einspeisungspunkten von Versorgungsunternehmen. Das sind zum Beispiel die Telefonanschlusskästen, die oft gleich neben den Mülltonnen stehen. Die leichte und für potentielle Angreifer relativ risikolose Zugänglichkeit der Datenleitungen erhöht die Gefahr, besonders dann, wenn der Wert der Daten einen Angriff auf das Rechnersystem lohnenswert erscheinen lässt.

Technisch ist das Anzapfen solcher Leitungen selbst für Laien kein Problem. Die Kosten für ein Analysegerät, mit dem die Kommunikationsdaten intelligent analysiert werden können, liegen zwischen 2 500 EUR und 5 000 EUR. Außerdem stehen im Internet zunehmend kostenlose Angriffstools zur Verfügung, mit denen »intelligente« Angriffe auf Rechnersysteme durchgeführt werden können.

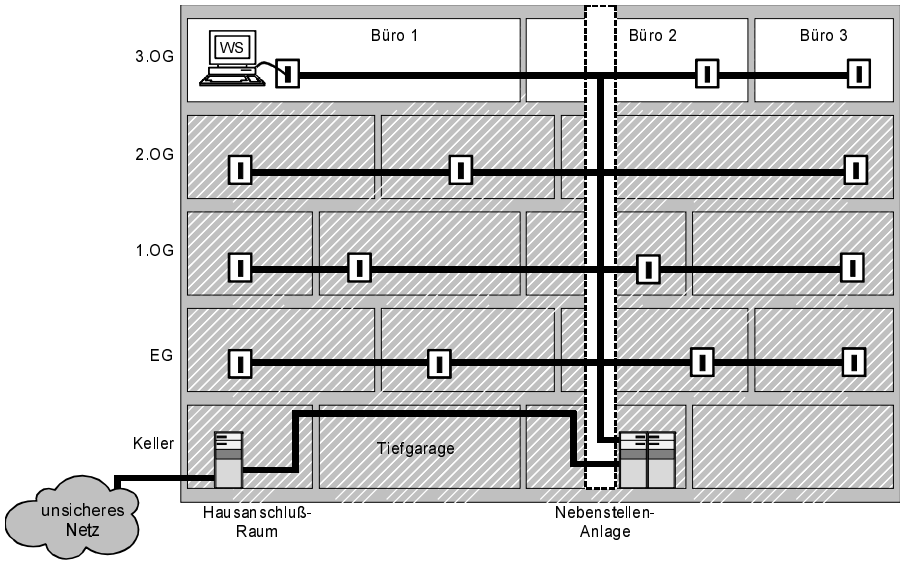

Abb. 3.11: Lokale Gegebenheiten, die das Angriffsrisiko erhöhen

Fazit

Die jeweiligen lokalen Gegebenheiten, die technische Machbarkeit und die relativ niedrigen Beschaffungskosten für Analysegeräte machen das Angriffsrisiko sehr hoch, vor allem, wenn der Angreifer sich davon ein lohnendes Geschäft versprechen kann.

Seit Jahren wächst die Computerkriminalität überdurchschnittlich. Da in den nächsten Jahren immer mehr Geschäftsprozesse über Rechner- und Kommunikations-Systeme abgewickelt werden, wird dieser Trend anhalten, wenn keine höheren Sicherheitsmaßnahmen eingeführt werden.

3.4 Schadenskategorien und Folgen

Um mögliche Schäden besser einschätzen zu können, werden nachfolgend einige typische Schadenskategorien erläutert /BSI99/. Diese beziehen sich auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.

3.4.1 Verstoß gegen Gesetze/Vorschriften/Verträge

Verstöße dieser Art können aus dem Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit resultieren. Die Schwere eines solchen Schadens ist dabei oftmals abhängig davon, ob es sich nur um einen Bagatellverstoß handelt, oder ob aus dem Vorgang rechtliche Konsequenzen für die Organisationen entstehen können. Zu den relevanten Gesetzen, Vorschriften und Verträgen gehören:

- Grundgesetz
- Bürgerliches Gesetzbuch
- Strafgesetzbuch (2. Wirtschaftskriminalitätsgesetz)
- Bundesdatenschutzgesetz und Datenschutzgesetze der Länder
- Sozialgesetzbuch
- Handelsgesetzbuch
- Telekommunikationsgesetz
- Personalvertretungsgesetz
- Betriebsverfassungsgesetz
- Urheberrechtsgesetz
- Patentgesetz
- Produkthaftungsgesetz
- Organisationsanweisungen und Dienstvorschriften
- Dienstleistungsverträge im Bereich Datenverarbeitung
- Verträge, die die Wahrung von Betriebsgeheimnissen vereinbaren
- Betriebsvereinbarungen
- EU-Recht
- Völkerrecht, bi- und multilaterale Abkommen

3.4.2 Beeinträchtigung der persönlichen Unversehrtheit

Die Fehlfunktion eines Rechnersystems kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen.

Beispiel:

- Verletzung einer Person durch Fehlfunktionen einer Produktionsmaschine aufgrund von Softwaremanipulation über das Internet

3.4.3 Beeinträchtigung der Aufgabenerfüllung

Gerade der Verlust der Verfügbarkeit eines Rechnersystems oder der Integrität von Daten kann die Aufgabenerfüllung in einer Organisation erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele:

- verzögerte Bearbeitung von Verwaltungsvorgängen,
- verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen,
- falsche Liefermenge aufgrund falscher Steuerungsdaten,
- unzureichende Qualitätssicherung durch Ausfall eines Mess-Systems.

3.4.4 Negative Außenwirkung

Durch den Verlust eines der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit in einem Rechnersystem können verschiedene negative Außenwirkungen entstehen, beispielsweise:

- Renommeeverlust einer Organisation,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Organisationen,
- Vertrauensverlust gegenüber einer Organisation,
- verlorenes Vertrauen in die Arbeitsqualität einer Organisation,
- Zuspielen vertraulicher Daten an die Presse oder die Konkurrenz,
- Einbuße der Konkurrenzfähigkeit.

Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes und am Verbreitungsgrad der Außenwirkung.

Ursachen für solche Schäden können vielfältiger Natur sein, unter anderem:

- Handlungsunfähigkeit einer Organisation durch Ausfall der IT-Systeme,
- fehlerhafte Veröffentlichungen durch manipulierte Daten,
- Fehlbestellungen durch mangelhafte Lagerhaltungsprogramme,
- Verstoß gegen die Schweigepflicht durch Vertraulichkeitsverlust von Daten.

Der mögliche Schaden durch eine negative Außenwirkung kann in vielen Organisationen sehr hoch sein.

3.4.5 Finanzielle Auswirkungen

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, durch die Veränderung von Daten oder durch den Ausfall eines Rechnersystems entstehen.

Beispiele:

- unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,
- Manipulation finanzwirksamer Daten in einem Abrechnungssystem,
- Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste,
- Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen.

Die Höhe des Gesamtschadens wird bestimmt durch die direkt entstehenden finanziellen Schäden und die daraus resultierenden pekuniären Folgeschäden.

3.5 Ergebnisse der KES/Utimaco-Studien

Die KES/Utimaco-Studien der Jahre 1996, 1998 und 2000 zeigen, wie der Status der Informationssicherheit in der betrieblichen Wirklichkeit in Deutschland ist. Die wichtigsten Ergebnisse finden sich konzentriert in /Görtz99/, wo folgende Fragen mit Blockdiagrammen aufgeschlüsselt sind:

- Welche Gefahren haben zu Beeinträchtigungen der IT-Sicherheit geführt?
- Wie ist die aktuelle Risikosituation in Unternehmen?
- Welche Probleme behindern die Verbesserung der Informationssicherheit?
- Wer ist für die Probleme der betrieblichen Informationssicherheit verantwortlich?
- Welche Maßnahmen werden zum Schutz der Kommunikation in öffentlichen Netzen angewandt?

3.6 Zusammenfassung

Mit dem enormen Anwachsen von Kommunikationsnetzen wie Internet und Intranets in der modernen Informationsgesellschaft wächst auch das Risiko, dass Daten manipuliert oder gestohlen werden können und dadurch ein Schaden auftritt.

Wir sind zwar nicht in der Lage, die Bedrohungen zu beeinflussen, aber wir können dafür sorgen, dass unsere Verletzbarkeit reduziert wird.

Aus diesem Grund wird es in Zukunft immer wichtiger, die Kommunikations-Systeme sicherer zu gestalten, damit eine vertrauenswürdige und beherrschbare Kommunikation realisiert werden kann.

Immer größere Bedeutung erlangen dabei aktive Abwehrmechanismen wie Security Audit-Systeme und Intrusion-Detection-/Response-Systeme. Schließlich können große Organisationen unmöglich ihren IT-Betrieb herunterfahren, nur weil jemand zum Beispiel an den Ports »fingert«.

Allerdings verbleibt trotz aller Sicherungsmaßnahmen immer noch ein kleines Restrisiko. Jede Organisation tut gut daran, Notfallpläne für den »Fall der Fälle« auszuarbeiten, in dem Verfahren und Zuständigkeiten festgelegt werden. Diese Pläne sollten von Zeit zu Zeit auch in einem Manöver getestet werden, um im Ernstfall Panik und damit unter Umständen zusätzlichen Schaden zu verhindern.

Ein abschließender Hinweis

In diesem Kapitel wurden prinzipiell die Gefahren aus dem Netz erklärt. Dies musste ohne Anspruch auf Vollständigkeit und Detailtiefe geschehen, sonst hätte es den Rahmen dieses Fachbuchs überschritten. Jeder Interessierte sollte sich bei Bedarf weiter informieren, beispielsweise in Web-Foren.

Besonders aktuell ist der 14-täglich verschickte »Security-Newsletter« aus dem INTEREST-Verlag. Er ist im Abonnement des »Organisationshandbuchs Netzwerksicherheit« enthalten und kann mit einem E-Mail-Warndienst kombiniert werden (siehe: `www.interest.de`).