X.systems.press

X.systems.press ist eine praxisorientierte Reihe zur Entwicklung und Administration von Betriebssystemen, Netzwerken und Datenbanken.

Roland Bless · Stefan Mink · Erik-Oliver Blaß
Michael Conrad · Hans-Joachim Hof
Kendy Kutzner · Marcus Schöller

Sichere Netzwerkkommunikation

Grundlagen, Protokolle und Architekturen

Mit 149 Abbildungen und 12 Tabellen

Springer

Roland Bless
Universität Karlsruhe
Institut für Telematik
Postfach 6980
76128 Karlsruhe
bless@sineko.de

Website zum Buch:
www.sineko.de

Stefan Mink
mink@sineko.de

Michael Conrad
conrad@sineko.de

Kendy Kutzner
kutzner@sineko.de

Erik-Oliver Blaß
blass@sineko.de

Hans-Joachim Hof
hof@sineko.de

Marcus Schöller
schoeller@sineko.de

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

ISSN 1611-8618
ISBN-10 3-540-21845-9 Springer-Verlag Berlin Heidelberg New York
ISBN-13 978-3-540-21845-9 Springer-Verlag Berlin Heidelberg New York

Springer ist ein Unternehmen von Springer Science+Business Media
springer.de

Umschlaggestaltung: KünkelLopka, Heidelberg
Satzerstellung durch die Autoren
Herstellung: LE-TEX Jelonek, Schmidt & Vöckler GbR, Leipzig
Gedruckt auf säurefreiem Papier 33/3142YL - 5 4 3 2 1 0

Für Iris, Dominik, Larissa, Juliane und Jannis
— R. B.

Für alle, die bei der Entstehung dieses Buches leiden mussten :)
— S. M.

Für Papa
— E.-O. B.

Für Sandra
— M. C.

Für Anika und meine Eltern
— H.-J. H.

Für Carola, Anita und Rolf
— K. K.

Für Andrea und Pascal
— M. S.

Vorwort

Dieses Buch beschäftigt sich mit Sicherheit in Netzwerken und entstand als gemeinsames Werk von sieben Autoren. Als Springer die Idee anregte, ein Buch über Netzwerksicherheit zu schreiben, fand dies schnell meine Zustimmung, da Netzwerksicherheit inzwischen ein sehr wichtiges Thema geworden ist, das viele Nutzer und Administratoren von Netzwerken betrifft. Dies gilt umso mehr, als wir sicher in Zukunft von noch mehr Netzwerkkonnektivität umgeben sein werden, aufkommende Personal Area Networks und Sensor/Aktor-Netze seien hier nur als Beispiel genannt.

Allerdings war auch klar, dass ich dieses Buch – als Freizeitprojekt – aus Zeitgründen nicht alleine würde schreiben können. Andererseits hatten die Kollegen Marcus Schöller und Stefan Mink bereits zweimal erfolgreich die Vorlesung Netzsicherheit am Lehrstuhl von Prof. Dr. Martina Zitterbart am Institut für Telematik der Universität Karlsruhe gestaltet und gehalten. Am Institut fanden sich somit schnell weitere Kollegen, die im Bereich Netzwerksicherheit über exzellentes Wissen verfügen und dieses gerne einbringen wollten. So wurde die Autorengruppe durch Erik-Oliver Blaß, Michael Conrad, Hans-Joachim Hof und Kendy Kutzner vervollständigt. Stefan Mink und ich übernahmen dabei zusätzlich die Editor-Aufgaben, was sicherlich bei einer so großen Autorengruppe und sehr unterschiedlichen Schreibstilen eine besondere Herausforderung ist. Die verbliebenen Unterschiede in den Formulierungen sind uns hoffentlich nachzusehen.

Als Freizeitprojekt hat dieses Buch allen Autoren sowie deren Familien oder Partnerinnen einige Opfer abverlangt. Hierfür möchte ich allen herzlich danken.

Inzwischen ist das Themengebiet der sicheren Netzwerkkommunikation so umfangreich geworden, dass in diesem Buch nicht einmal sämtliche Themen erschöpfend behandelt werden konnten. So wurden beispielsweise Sicherheitsbetrachtungen zu Mobile IP, Multicast, HIP (Host Identity Protocol), Sensornetzen usw. vorerst nicht mit aufgenommen, u. a. weil uns einige Themen

weniger praxisrelevant als andere erschienen. Wer gleich einen Blick in das Inhaltsverzeichnis wirft, wird feststellen, dass es vor Abkürzungen nur so wimmelt. Leider konnten wir das Problem nicht umgehen, denn die Verfahren und Protokolle werden in der Praxis häufiger unter ihrer Abkürzung als unter der ausgeschriebenen Bezeichnung genannt. Wir hoffen aber, dies durch ein umfangreiches Abkürzungsverzeichnis einigermaßen kompensiert zu haben.

Bei aller erdenklichen Sorgfalt während der Erstellung des Buches können sich trotzdem einige Fehler eingeschlichen haben. Wir bieten im WWW unter der URL http://www.sineko.de/ eine Seite mit Errata und Neuigkeiten zum Buch an und freuen uns über Rückmeldungen.

Wir wünschen allen Lesern – trotz des ernsten Stoffs – viel Spaß mit diesem Buch!

Karlsruhe,
April 2005 *Roland Bless*

Inhaltsverzeichnis

1

Einleitung

Netzwerke sind in der Informationstechnik (IT) ein besonders wichtiges Element geworden. Durch den großen Erfolg des Internets und die damit verbundenen Kommunikationsprotokolle werden in Firmen zahlreiche IT-Prozesse inzwischen über Internet-basierte Netzwerke abgewickelt: teilweise nur intern innerhalb eines Standorts, teilweise aber auch standortverbindend oder sogar zur Kommunikation mit Kunden und Geschäftspartnern. Netzwerke werden somit immer häufiger Bestandteil kritischer Infrastrukturen. Der Ausfall oder der Verlust der Vertraulichkeit, Integrität oder Authentizität der internen Kommunikation kann einen sehr großen Schaden für die jeweilige Institution bedeuten.

1.1 Motivation

Neben der steigenden Vernetzung in der Wirtschaft nimmt der Trend zur Vernetzung aber auch im Privatbereich zu: Heim-PCs werden bereits standardmäßig mit Kommunikationstechniken wie Wireless LAN und Ethernet ausgeliefert und verfügen immer häufiger über eine permanente Verbindung ins Internet (z. B. mittels einer DSL-Flatrate). Die zunehmende Konnektivität von Rechnern bringt zwar zahlreiche Vorteile mit sich, birgt aber auch Gefahren, da ein Angreifer nun keinen direkten physikalischen Zugang zu einem Rechner mehr haben muss. Ein Angreifer versucht so beispielsweise über das Netzwerk in den Rechner einzudringen und ihn unter seine Kontrolle zu bekommen oder seinen Betrieb zu stören bzw. seinen Ausfall herbeizuführen. Inzwischen verfolgen solche Angreifer zunehmend kommerzielle Interessen, so kompromittieren sie z. B. gegen Bezahlung Rechner zu Zwecken des unautorisierten Versendens von unverlangter Werbung per E-Mail, so dass ein stetiger Anstieg solcher Angriffe wenig verwunderlich ist. Die Gefährdung der Sicherheit von Rechnern durch Vernetzung ist daher recht groß und wird vermutlich weiter steigen.

Die Kenntnis über Sicherheit (im Sinne von „Security“) in Netzwerken wird dadurch zunehmend wichtiger, wenn nicht inzwischen sogar unentbehrlich. Sicherheitsrelevante Fragen, die auch normale Endanwender betreffen, sind beispielsweise: „Ist der Online-Banking-Server tatsächlich derjenige von meiner Bank oder gibt sich der Rechner eines Angreifers als mein Bankserver aus?“ oder „Liest jemand den Inhalt meiner E-Mails bei der Übertragung?“ sowie „Ist mein Wireless LAN vor unbefugtem Zugriff sicher?“. Netzwerkadministratoren beschäftigen unter anderem Fragen wie: „Wie können unberechtigte Zugriffe von außen auf das Netzwerk verhindert werden?“ oder „Ist die Kopplung der Netzwerke zwischen unseren Standorten wirklich sicher vor Angreifern, die Kommunikationsdaten abhören oder manipulieren wollen?“.

Der Einsatz und die Wahl geeigneter Sicherheitsmechanismen hängt von vielen Aspekten ab, weshalb es durchaus gefährlich sein kann, blindlings vermeintlichen „Patentrezepten“ zu folgen. Sicherheit ist komplex und facettenreich. Neben der Festlegung des individuellen Schutzbedarfs ist es daher wichtig, über das notwendige Hintergrundwissen zu verfügen und umsichtig bei der Wahl von Sicherheitsmechanismen vorzugehen. Die Vielzahl von Möglichkeiten zur Sicherung von Netzwerken stellt Netzwerkadministratoren und Endanwender gleichermaßen vor das Problem, die sinnvollste Kombination von Sicherheitstechniken für den jeweiligen Einsatzzweck auszuwählen. Dieses Buch konzentriert sich auf *Netzwerksicherheit*, vor allem im Bereich der Internet-Protokollwelt. Es beschreibt sowohl Sicherheitsrisiken und Gefährdungen, die bei der Benutzung ungesicherter Kommunikationsprotokolle bestehen, als auch Protokolle und Architekturen, die eine sichere Netzwerkkommunikation ermöglichen.

Wie bei vielen anderen Bereichen in der Informatik gilt es auch und insbesondere beim Thema Sicherheit, sich ständig über neue Entwicklungen zu informieren. Werden beispielsweise Schwächen in grundlegenden Sicherheitsalgorithmen – wie z. B. erst kürzlich im Hash-Algorithmus SHA-1 – entdeckt, so hat dies meistens weitreichende Konsequenzen auf bereits vorhandene Sicherheitslösungen. Vorher als sicher geltende Verfahren sind durch neu gewonnene Erkenntnisse unter Umständen nicht mehr ausreichend sicher. Daher ist anzunehmen, dass einige der in diesem Buch beschriebenen – und vom heutigen Standpunkt aus als sicher geltende – Sicherheitsverfahren im Laufe der Zeit unsicher werden können.

1.2 Sicherheit im Internet

Heutige Internet-basierte Netzwerke sind in vielerlei Hinsicht in hohem Maße unsicher, sofern keine weiteren Sicherungsmaßnahmen getroffen werden. Die Ursachen hierfür liegen hauptsächlich darin begründet, dass in der Zeit der Spezifikation dieser Protokolle noch ein anderes Vertrauensmodell existierte

und Sicherheitsmechanismen immer einen gewissen Mehraufwand bedeuten, der ohne wohlbegründeten Schutzbedarf meistens nicht in Kauf genommen wird. In den Anfängen des Internets wurde es hauptsächlich von einer kleineren Gemeinde technisch versierter Teilnehmer genutzt, die einander vertrauten und beispielsweise Angriffe auf die Verfügbarkeit von Kommunikationsdiensten als unlogisch und schädigend betrachteten.

Im Unterschied zur damaligen Situation dient das Internet heutzutage weitgehend dazu, um Organisationen und Personen miteinander zu verbinden, die sich gegenseitig zunächst nicht vertrauen, aber z. B. dennoch Geschäftsvorgänge, u. a. Warenbestellungen und Bezahlvorgänge, über das Internet abwickeln wollen. Inzwischen hat sich also auch die Teilnehmerstruktur weitgehend geändert, so dass sich durch die früher entworfenen und flexiblen Mechanismen heutzutage Probleme wie das massenhafte Versenden unerwünschter Werbe-E-Mails („SPAM“) ergeben, was von den ursprünglichen Entwicklern des E-Mail-Transportsystems zum damaligen Zeitpunkt nicht vorausgesehen wurde.

Auch wenn das Thema dieses Buches vornehmlich die sichere Netzwerkkommunikation darstellt, gibt es einige weitere Aspekte, die für das Verständnis und die Betrachtung der Gesamtsicherheit wichtig sind, so dass diese im Folgenden zumindest angesprochen werden, wenngleich sie aus Platzgründen nicht ausführlich behandelt werden können.

1.3 Abgrenzung

Einbrüche in Rechner oder Netzwerkelemente wie Router durch Ausnutzung von Sicherheitslücken in Betriebssystemimplementierungen sind nicht Gegenstand dieses Buches, obwohl diese praktisch eine sehr wichtige Rolle spielen und in einem Sicherheitskonzept unbedingt berücksichtigt werden müssen. Solche Lücken entstehen durch fehlerhafte und damit wenig robuste Implementierungen, so dass diese Schwächen gezielt für Angriffe ausgenutzt werden, um in Rechner einzudringen. Es ist davon auszugehen, dass solche Fehler immer in Teilen der Betriebssysteme (also auch in Implementierungen von Netzwerkprotokollen) oder in Anwendungen vorhanden sein werden, insbesondere vor dem Hintergrund der zunehmend komplexer werdenden Softwaresysteme. Solche implementierungsbedingten Sicherheitslücken lassen sich aber im Gegensatz zu protokoll-inhärenten Sicherheitsproblemen beheben, meist durch Einspielen von so genannten *Patches*, welche gezielt die bekannt gewordenen Sicherheitsprobleme beseitigen. Andererseits macht keine noch so sichere Implementierung ein Protokoll sicher, das von der Konzeption her Schwächen aufweist.

Dem Leser sollte überdies immer bewusst sein, dass es absolute Sicherheit praktisch nicht gibt, weil jeder Sicherheitsmechanismus überwindbar ist, denn

meistens ist es nur eine Frage des Aufwands, um den Schutz zu überwinden. Der konkrete Aufwand bezieht sich in den meisten Fällen auf den für Rechenoperationen zu leistenden Zeitaufwand. Außerdem sind vermeintlich sichere kryptographische Verfahren nur so lange als sicher anzusehen, wie keine Schwächen oder Sicherheitslücken aufgezeigt und nachgewiesen wurden. Eine Offenlegung und Prüfung solcher Verfahren durch ausgewiesene Sicherheitsexperten – so genannte Kryptoanalytiker – ist daher unerlässlich.

1.4 Faktor Mensch

Gefährdungen der Sicherheit drohen aber auch für bislang ungebrochene Verfahren von anderer Seite: Der Faktor Mensch trägt häufig durch die Wahl schwacher, d. h. leicht zu erratender Passwörter dazu bei, dass der Schutz unzureichend wird. Eine andere Methode, das Passwort „zu brechen“, ist, den Benutzer dazu zu überreden, es unwissentlich zu verraten. So werden in letzter Zeit von Angreifern verstärkt Methoden eingesetzt, die unachtsame oder leichtgläubige Benutzer zur Herausgabe ihrer Zugangskennungen und Passwörter anhand nachgeahmter Web-Seiten oder E-Mails bewegen (so genanntes *Password Fishing*, kurz *Phishing*). Nicht selten führt auch menschliche Bequemlichkeit dazu, dass sich Benutzer nicht an geltende Sicherheitsvorgaben halten, weil Sicherheitsmaßnahmen oft als lästig empfunden werden. Es ist daher auch immer abzuwägen, was man durch den Einsatz von Sicherheitsmaßnahmen aufgibt im Vergleich zum Gewinn an Sicherheit, wie Bruce Schneier ausführlich in seinem Buch „Beyond Fear“ darlegt [335]. Schließlich werden zivile Personen auch keine schusssichere Weste ohne weitere Veranlassung tragen, nur weil es grundsätzlich sicherer ist.

Manchmal werden auch Sicherheitsmechanismen eingeführt, die zwar für ihren Einsatzzweck als absolut sicher gelten, jedoch an anderer Stelle umgangen werden können. Fehlplatzierte Sicherungsmaßnahmen sind daher ähnlich unnütz wie teure, gegen Einbruch gesicherte Fenster wenn die Eingangstür weit offen steht. Es lassen sich zahlreiche Beispiele hierfür anführen: Untergeschobene und bösartig modifizierte Programme (so genannte *Trojaner*), welche Tastatureingaben mitprotokollieren, können sogar auch gut gewählte Passwörter für sichere Verfahren abhören, um z. B. private Schlüssel auszuspionieren. Weitere Beispiele sind Funktastaturen deren Signal abgehört werden kann oder der Gebrauch eines Notebooks im Zug oder Flugzeug, das von in der Nähe sitzenden Personen eingesehen werden kann und ggf. mit Digital-Kameras abfotografiert werden kann. Firewalls bieten oftmals nur einen Schutz eines Netzwerks gegen Angriffe von außen, sind jedoch recht wirkungslos, wenn ein Mitarbeiter ein mit Würmern infiziertes Notebook von einer Konferenz anschließend wieder mit dem Intranet verbindet und so das Netzwerk von innen heraus infiziert. Zudem darf nicht vernachlässigt werden, dass Sicherheit manchmal als Behinderung empfunden wird, so dass dann oftmals Wege gesucht werden, um

die Sicherheitsmechanismen zu umgehen. Als Beispiel sei ein Bankmitarbeiter genannt, der eine ISDN-Karte in seinen Arbeitsplatzrechner eingebaut hat, um auch vom Arbeitsplatz aus das Internet nutzen zu können, wodurch eine nicht vorgesehene Verbindung des Intranets mit dem Internet entstand.

Ein wichtiger Prozess ist daher, die Sicherheitsziele zu definieren und die Nutzung dazu passende Sicherheitsmechanismen festzulegen. Dies ist durchaus auch die Aufgabe der Leitungsebene eines Unternehmens. Prinzipiell muss die Festlegung des Schutzbedarfs für jeden Einzelfall geschehen, was sehr aufwändig werden kann. Andererseits gibt es aber auch allgemeine Empfehlungen wie z. B. das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) [53], das als sinnvolle Basis dienen kann.

Zu guter Letzt sei noch darauf hingewiesen, dass ein nicht unbeträchtlicher Teil von Sicherheitsvorfällen durch „Innentäter“ verursacht werden, weshalb auch ein Schutz besonders kritischer Infrastrukturen vor dem Zugriff durch eigene Mitarbeiter berücksichtigt werden muss. Des Weiteren sind in einer Planung auch Notfallpläne zu definieren und ggf. zu proben.

1.5 Gliederung des Buches

Dieses Buch ist in mehrere Teile untergliedert. In Teil I werden Grundlagen zur Sicherheit vorgestellt. In Kapitel 2 wird zunächst mit Erläuterungen zur allgemeinen Systemsicherheit fortgefahren und Kapitel 3 beschreibt kryptographische Mechanismen, die als Grundlage für die meisten Sicherheitsmechanismen dienen, die in Teil II vorgestellt werden. Dieser Teil beginnt mit einer Beschreibung allgemeiner Sicherheitsmechanismen in Kapitel 4. Anschließend werden konkrete Sicherheitsmechanismen für Protokolle sowie Sicherheitsprotokolle und -architekturen in Reihenfolge der unterschiedlichen funktionalen Protokollschichten vorgestellt, d. h. Netzzugangsschicht, Netzwerkschicht, Transportprotokollschicht und Anwendungsschicht. Eine gewisse Ausnahme bildet Kapitel 8, das sich mit der Sicherheit der Netzwerkinfrastruktur beschäftigt, mit deren Verwaltung Kommunikationsteilnehmer normalerweise nicht unmittelbar konfrontiert werden. Teil III erläutert den Einsatz und das Zusammenspiel einiger der in Teil II vorgestellten Sicherheitsmechanismen anhand einiger typischer Szenarien.

Teil I

Grundlagen

2

Systemsicherheit

Auch wenn dieses Buch sich vornehmlich mit Netzwerksicherheit beschäftigt, müssen weitere Sicherheitsaspekte immer zusätzlich beachtet werden, denn Sicherheit in Netzwerken kann praktisch nicht isoliert, z. B. unabhängig von Endsystemsicherheit oder der gesamten Sicherheitsstrategie einer Institution, betrachtet werden. Netzwerksicherheit wird in der Praxis nur einen Teil eines ganzheitlichen Sicherheitskonzepts darstellen. Bevor sich dieses Buch also näher mit Sicherheit in Kommunikationsnetzen befasst, müssen der Vollständigkeit halber noch einige Begriffe und Sachverhalte aus dem Bereich Sicherheit und Netzwerke im Allgemeinen vorgestellt und erwähnt werden, die allerdings im Rahmen des Buchs nicht erschöpfend behandelt werden können. Daher befasst sich dieses Kapitel mit den eher allgemeinen Aspekten der *Systemsicherheit*.

Zunächst wird motiviert, weshalb Sicherheit eine wichtige Managementaufgabe darstellt, was Sicherheitsrichtlinien beinhalten und in welchem Verhältnis sich Sicherheit zu verwandten Aspekten wie Robustheit und Fehlertoleranz befindet. Anschließend werden allgemeine Bedrohungen und Sicherheitsziele beschrieben, wonach dann speziell Sicherheitsziele in Netzwerken erläutert werden. Das für die Einordnung von Sicherheitsmechanismen wichtige Schichtenmodell für Kommunikationssysteme wird in Abschnitt 2.7 beschrieben, wonach noch kurz Endsystemsicherheit im Allgemeinen und einige Details zu Denial-of-Service-Angriffen betrachtet werden.

2.1 Sicherheit als Managementaufgabe

Der Begriff *Sicherheit* hat für verschiedene Betrachter sehr unterschiedliche Bedeutungen. Sicherheit kann beispielsweise bedeuten:

- Daten nur für eine begrenzte und wohldefinierte Menge von Personen zugänglich zu machen

- die Vertraulichkeit von Daten zu schützen
- Anonym zu kommunizieren
- Daten vor Verfälschung zu sichern
- Kommunikationsvorgänge abzuhören, um Terroristen zu fangen

Manche Vorstellungen oder Ziele von Sicherheit sind offensichtlich widersprüchlich: Während die meisten Kommunikationsteilnehmer einen vertraulichen Datenaustausch wünschen, möchten einige Staatsorgane Zugang zu beliebigen Kommunikationsvorgängen erhalten, z. B. zum Zwecke der Verbrechensbekämpfung. Es gilt also bei der Behandlung des Themas immer genau zu definieren, was unter Sicherheit verstanden wird und welche Sicherheitsziele verfolgt werden. Diese Punkte sind daher wesentlicher Gegenstand von Abschnitt 2.4.

Folgende Aspekte sind grundsätzlich zu berücksichtigen und zu entscheiden:

- Welche Sicherheitsziele sollen überhaupt verfolgt werden?
- Wer legt die Sicherheitsziele fest?
- Wer setzt sie um?
- Wer kontrolliert die Einhaltung der Sicherungsmaßnahmen?

Die Feststellung des Schutzbedarfs und des Sicherheitsniveaus sowie die Festlegung der Sicherheitsmaßnahmen sind insbesondere Aufgaben der obersten Leitungsebene von Unternehmen oder Einrichtungen. Schließlich können Sicherheitsdefizite weitreichende (letztlich vor allem finanzielle) Konsequenzen haben, derer sich das Management bewusst sein muss. Fehlende Sicherheit kann bei sicherheitsrelevanten Vorfällen beispielsweise zu Produktionsausfall, Imageverlusten, Vertrauensverlust bei Kunden oder Geschäftspartnern und somit schließlich zu einem Umsatzrückgang oder Einnahmeausfall führen. Das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG) in Deutschland verlangt daher, dass eine Analyse für solche Risiken und deren Auswirkungen auf die anderen Geschäftsbereiche erfolgen muss. Manchmal wird dennoch erst über Sicherheitskonzepte und -vorkehrungen nachgedacht, wenn ein Schaden durch einen Sicherheitsvorfall eingetreten ist. Angesichts des eingetretenen Schadens und des damit unmittelbar sichtbar gewordenen Risikos, ist es andererseits dann relativ einfach, die Bereitstellung der erforderlichen Mittel für entsprechende Sicherheitsmaßnahmen zu motivieren. Der Totalausfall des Standorts eines Telefonmehrwertdienstes (z. B. 0900er-Sondernummern) über mehrere Stunden oder gar Tage dürfte dem Betreiber der Plattform einen so großen Einnahmeausfall bescheren, dass beispielsweise die Kosten für den Aufbau und Unterhalt eines weiteren zusätzlichen und örtlich getrennten Standorts relativ gering erscheinen. Zusätzliche Systeme als

Redundanz zur Steigerung der Ausfallsicherheit bedeuten aber auch weitere Angriffspunkte, die wie die Primärsysteme gleichermaßen gesichert werden müssen.

Schließlich erfordert die Durchsetzung und Kontrolle der Sicherheitskonzepte und -maßnahmen einen nicht unerheblichen zeitlichen, personellen und materiellen Aufwand. Die Sensibilisierung der Vorgesetzten und insbesondere der Leitungsebene für Sicherheitsmaßnahmen ist für die technischen Verantwortlichen im Vorfeld manchmal ein mühsames Unterfangen. Das liegt zum einen daran, dass die Beurteilung der Bedrohungen, Risiken und damit des Schutzbedarfs in Abhängigkeit des Betrachters sehr unterschiedlich ausfallen kann. Zum anderen mögen Sicherheitsmaßnahmen nutzlos erscheinen oder gar als Behinderung empfunden werden, wenn keine Sicherheitsvorfälle eintreten.

Weitere zu berücksichtigende Aspekte sind u. a. das Benutzerverhalten (z. B. in Bezug auf Bequemlichkeit, Gewohnheiten und Vorlieben), die Akzeptanz und Durchsetzung der Sicherheitsmaßnahmen sowie physikalische Maßnahmen wie Schließsysteme und Zugangskontrollen. In Zusammenhang mit letzteren sollte man auch daran denken, dass Personen wie Reinigungspersonal oder Hausmeister meistens unbeschränkten Zugang zu Räumlichkeiten haben, so dass eine Absicherung der Systeme an sich vor Ort nach wie vor notwendig ist.

Wie zuvor motiviert, sollten aufgrund der weitreichenden Konsequenzen so wichtige Entscheidungen wie das Festlegen der Sicherheitsziele und das Definieren der Sicherheitsrichtlinien Managementaufgaben sein. Sicherheitsrichtlinien sind Gegenstand des folgenden Abschnitts.

2.2 Sicherheitsrichtlinien

Sicherheitsrichtlinien definieren Regeln, die in Bezug auf bestimmte Sicherheitsaspekte befolgt werden müssen. Da diese Vorgaben größtenteils auf politischen Entscheidungen (d. h. oftmals nicht-technischer Argumente) basieren, ist auch der Begriff *Sicherheitspolitik* (engl. *Security Policy*) gebräuchlich. Das Festlegen von Verantwortlichkeiten gehört genau so dazu wie eine Konsolidierung der Sicherheitsrichtlinien. Die Umsetzung der Sicherheitskonzepte muss durch regelmäßige Sicherheitsaudits ebenso überprüft werden wie die Einhaltung der Sicherheitsrichtlinien. Dementsprechend müssen sie auch Maßnahmen enthalten, die einen Verstoß gegen die Sicherheitsrichtlinien ahnden. Werden beispielsweise unerlaubte Datenverbindungen (z. B. unter Nutzung eines Mobiltelefons zur Datenübertragung) aus einem geschützten Netzwerk heraus initiiert, kann das die Sicherheit des gesamten Netzwerks gefährden, da plötzlich ein nicht-kontrollierter Übergang in ein anderes, öffentliches Netzwerk entsteht.

Die Festlegung von Verantwortlichkeiten, die Vergabe von Zutritts-, Zugangsberechtigungen und Zugriffsrechten sowie die Regelung des Passwortgebrauchs sind ebenfalls Gegenstand von Sicherheitsrichtlinien (vgl. auch Maßnahmenkataloge im BSI-Grundschutzhandbuch [53]), die durch das IT-Sicherheitsmanagement getroffen werden müssen. Darüberhinaus gibt es auch entsprechende technische Umsetzungen einiger Sicherheitsrichtlinien, z. B. als so genannte *Security Policy Database* in IPsec-Implementierungen (vgl. Abschnitt 6.2.6, S. 223) oder als Paketfilterregeln in einer Firewall (vgl. Abschnitt 6.6, S. 253).

Weitere allgemeine und speziellere Überlegungen zum Vorgehen bei Festlegung von Security Policies in Bezug auf Netzwerke liefern beispielweise [128, 142].

2.3 Robustheit und Fehlertoleranz

Zuverlässigkeit und Robustheit der Systeme sind weitere Gesichtspunkte, die im Kontext der Sicherheit ebenfalls eine besondere Rolle spielen. Schließlich drohen Gefahren für die Sicherheit eines Systems nicht nur durch vorsätzliche Beeinträchtigung durch Angreifer sondern auch durch unabsichtliche Beeinträchtigung, beispielsweise durch menschliches Versagen bei der Bedienung oder Konfiguration von Geräten. Der Schwerpunkt des Buches liegt jedoch deutlich auf vorsätzlichen Handlungen, welche die Sicherheit gefährden.

Für die Feststellung des Schutzbedarfs ist es ist also hilfreich, Überlegungen für den Fall anzustellen, dass bestimmte Teile der Infrastruktur oder von ihr erbrachte Dienste für längere Zeit nicht verfügbar sind. Welche Konsequenzen hat der stunden- oder tagelange Ausfall einzelner Systeme? Ist die Produktion gefährdet oder müssen Mitarbeiter in Zwangsurlaub entlassen werden, weil sie für ihre Arbeit auf die Infrastruktur angewiesen sind?

Oftmals findet man durch eine entsprechende Analyse der Infrastruktur eine inadäquate Sicherung bestimmter Systeme: einige Systeme sind möglicherweise gegen Ausfall abgesichert, obwohl deren Absicherung alleine aber nicht hinreichend ist, falls bereits davorliegende Systeme ausgefallen sind. So kann beispielsweise ein redundant ausgelegter Server nicht abhelfen, falls davorliegende Netzkomponenten wie Switches oder Router ausfallen, die nicht entsprechend redundant ausgelegt wurden. Zusätzlich gilt es auch die Stromversorgung, Klimatisierung und Leitungsführung miteinzubeziehen. Redundante Anlagen innerhalb des gleichen Gebäudes sind möglicherweise ebenso von einem Ausfall betroffen, falls nur eine Zuleitung für das Netz existiert und diese durch den oft zitierten „Bagger“ bei Bauarbeiten zerstört wird. Es ist daher durchaus wichtig, diese Abhängigkeiten zu identifizieren und die Unternehmensführung in Entscheidungen einzubinden, um entsprechende präventive Sicherheitsmaßnahmen einzuleiten. Andererseits kann auch eine Sicherung eines Teilsystems unnötig sein und nicht zur Steigerung der Sicherheit eines

Gesamtsystems beitragen, weil möglicherweise nur wenig sicherheitsrelevante Teile des Gesamtsystems durch das Teilsystem erbracht werden, wodurch sich der Schutzbedarf des Teilsystems relativiert.

2.4 Allgemeine Bedrohungen und Sicherheitsziele

Zur Beurteilung, Herstellung oder Verbesserung der Sicherheit eines Kommunikationssystems muss zunächst der *Schutzbedarf* ermittelt werden. Dazu ist es notwendig, *Sicherheitsziele* zu definieren und *Bedrohungen* derselben zu betrachten. Unter Bedrohung versteht man die Gefährdung eines oder mehrerer Sicherheitsziele durch mögliche Angriffe. Ein Angriff stellt daher die konkrete Realisierung einer Bedrohung dar. So kann beispielsweise die *Vertraulichkeit* der Kommunikation zwischen zwei Kommunikationspartnern A und B, in den folgenden Beispielen – wie in der Kryptographie üblich – meist stellvertretend mit *Alice* und *Bob* bezeichnet, durch einen Angreifer – mit *Eve* (aus dem Englischen *Eavesdropper*) bezeichnet – bedroht werden, wenn es ihm gelingt, Zugriff auf das Kommunikationsmedium zu bekommen (vgl. Abbildung 2.1). Hierbei wird bereits deutlich, dass die Bedrohung in Abhängigkeit der Kommunikationsform bzw. des Kommunikationskanals unterschiedlich ausfallen kann: Kommunizieren Alice und Bob per Telefon, könnte der Angreifer beispielsweise den technischen Kommunikationsweg angreifen; eine Installation von Mikrofonen am Aufenthaltsort von Alice und Bob wäre eine weitere Möglichkeit. Kommunizieren die beiden per ungesicherter E-Mail, könnte ein Angreifer z. B. auch einen auf dem Kommunikationspfad liegenden kompromittierten Mail-Server zum Mitlesen verwenden.

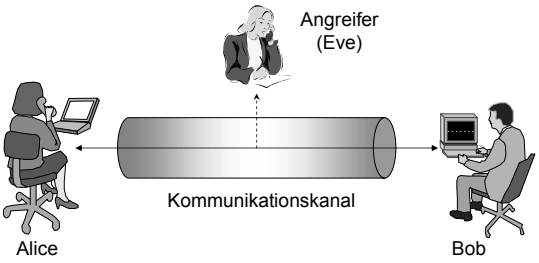

Abbildung 2.1. Kommunikationskanal zwischen Alice und Bob, bedroht durch Angreifer

Wie bereits eingangs erwähnt, ergeben sich oftmals auch widersprüchliche Sicherheitsziele: Während man sich selbst die Bewahrung der Vertraulichkeit und Privatsphäre während einer Kommunikation wünscht, möchten Unternehmen oder Regierungen im Gegensatz dazu häufig kontrollieren oder er-

fahren, welche Informationen ausgetauscht werden. Ein weiteres Beispiel ist die Anfertigung und Verteilung von Schlüsselkopien, um sich vor eventuellem Datenverlust zu schützen. Wer hat im wirklichen Leben nicht selbst schon Nachbarn eine Kopie des eigenen Wohnungsschlüssels anvertraut, weil er das Risiko eines Missbrauchs durch dieselben im Vergleich zum Verlust oder Vergessen des Schlüssels als relativ gering einschätzte?

2.5 Bedrohungsszenarien und Angriffe

Für eine Kommunikationsbeziehung zwischen zwei *Instanzen* (z. B. Personen, Anwendungen oder Rechnern) existieren im Allgemeinen verschiedene Bedrohungen, die in den folgenden Abschnitten beschrieben werden.

2.5.1 Abhören

Ein Angreifer hört einen Kommunikationsvorgang anderer Instanzen ab, wobei er Kommunikationsdaten mitliest, die nicht für ihn bestimmt sind. Je nach Art des eingesetzten physikalischen Mediums variieren Schwierigkeitsgrad und Aufwand für diesen *passiven*, d. h. nicht aktiv in die Kommunikation eingreifenden, Angriff. Drahtlose Medien wie Funkübertragungsstrecken sind in der Regel einfach, optische Medien wie Glasfasern sind dagegen deutlich aufwändiger abzuhören. Neben dem Verlust der Vertraulichkeit der Daten können sich hierdurch weitere Angriffsmöglichkeiten ergeben. Beispielsweise können u. U. durch Abhören Zugangsberechtigungsdaten wie Passwörter in Erfahrung gebracht werden, die für weitere Angriffe wie das Eindringen in Systeme, benutzt werden können.

Selbst wenn der Nutzdateninhalt verschlüsselt sein sollte, können die in Protokollköpfen vorhandenen Adressinformationen ausreichen, um eine *Verkehrsanalyse* (manchmal auch als Verkehrsflussanalyse bezeichnet) zu erstellen, die untersucht, wer mit welchen Kommunikationspartnern zu welchen Zeitpunkten wie lange kommuniziert. Diese Kenntnis reicht häufig schon aus, um recht genau auf Beziehungen und das Umfeld der beobachteten Kommunikationsteilnehmer schließen zu lassen. Aus den Zeitpunkten und der Reihenfolge der Kommunikationsvorgänge lassen sich häufig bereits bestimmte Sachverhalte erschließen.

Das Abhören ist normalerweise ein passiver Angriff, da die übermittelten Daten nicht verändert werden. Dies gilt allerdings nicht für neuartige Übertragungskanäle, die auf *Quantenkryptographie* aufbauen. Diese Kanäle gelten derzeit als abhörsicher, da ein Abhören in diesem Fall eine Veränderung der übertragenen Daten bewirkt, so dass der Abhörvorgang bemerkt werden kann. Diese Techniken besitzen momentan noch eine relativ geringe Bitrate, so dass

dieser abhörsichere Kanal vorerst nur für einen sicheren Schlüsselaustausch eingesetzt wird, bei dem kleinere Datenmengen fließen.

2.5.2 Einfügen, Löschen oder Verändern von Daten

Ein Angreifer erzeugt neue Daten, fängt Daten ab, vernichtet oder verändert sie. Im Unterschied zum passiven Abhören greift hier der Angreifer aktiv in die Kommunikation ein, d. h. er benötigt auch einen schreibenden Zugriff auf das Kommunikationsmedium. Typischerweise hat ein Angreifer, der sich zwischen die Kommunikationsteilnehmer schaltet (ein so genannter *Man-in-the-Middle*), weitreichende Möglichkeiten auf den Kommunikationsvorgang Einfluss zu nehmen. Beispielsweise kann ein solcher Angreifer den Kommunikationsteilnehmern die Identität des jeweils anderen Teilnehmers vorspielen (vgl. Maskerade) und Daten beliebig abfangen, zerstören, verändern oder wiedereinspielen (vgl. Abbildung 2.2).

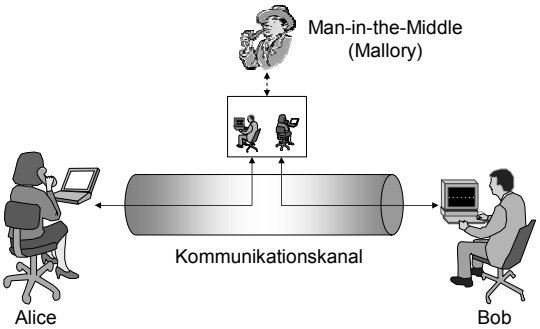

Abbildung 2.2. Man-in-the-Middle-Angriff auf den Kommunikationskanal zwischen Alice und Bob

Im Unterschied zur Modifikation von existierenden Daten werden beim Fälschen bzw. Einfügen von Daten *neue* Daten von einer Instanz unter Vorspiegelung der Identität einer anderen Instanz erzeugt.

2.5.3 Verzögern und Wiedereinspielen von Daten

Eine angreifende Instanz verzögert Daten, indem sie zunächst die Daten abfängt und erst zu einem späteren Zeitpunkt weiterleitet. Kommunikationsvorgänge, die zeitlichen Abhängigkeiten unterworfen sind, können hierdurch gezielt gestört werden. Beispielsweise könnten Angebote eines Konkurrenten

so lange aufgehalten werden, bis die entsprechende Frist abgelaufen ist oder Aktienverkäufe bei fallendem Kurs unnötig verzögert werden.

Ein *Wiedereinspielungsangriff* (auch als *Replay-Attacke* bezeichnet) besteht darin, Daten abzuhören und später erneut einzuspielen. Im Gegensatz zum Verzögerungsangriff bleibt ein Wiedereinspielungsangriff zunächst ohne Einfluss auf den eigentlichen Kommunikationsvorgang. Das Wiedereinspielen kann zu einem u. U. sehr viel später gelegenen Zeitpunkt erfolgen. Die Auswirkungen eines solchen Angriffs können in Abhängigkeit des Kommunikationsvorgangs sehr unterschiedlich sein, je nachdem ob Zugangsberechtigungen oder bestimmte Anwendungsaktionen davon betroffen und nicht gegen Wiedereinspielen geschützt sind.

2.5.4 Maskerade

Eine Instanz gibt vor, die Identität einer anderen Instanz zu besitzen. Eine Maskerade kann zur Vorbereitung weiterer Angriffe eingesetzt werden, beispielweise zur Beschaffung von Zugangsberechtigungen, um anschließend in Systeme einzudringen oder Dienste unautorisiert zu nutzen. Ein prominentes Beispiel für einen Maskerade-Angriff ist das in jüngster Zeit populär gewordene so genannte *Phishing* (von *Password Fishing*), welches unter Verwendung von echten Logos, Schriftzügen usw. durch eine nahezu authentisch wirkende E-Mail den Empfänger dazu verleitet, Zugangsberechtigungsdaten (z. B. Kontonummer, PIN und TAN für Bankverbindungen) preiszugeben.

Ein weiteres Beispiel für eine Maskerade ist die Fälschung der Absendeadresse in IP-Datenpaketen, um die Rückverfolgung des Angreifers zu erschweren. Maskerade wird aber auch von Programmen eingesetzt, deren Gattung als *Trojanische Pferde* (oder kurz *Trojaner*) bezeichnet wird (vgl. Abschnitt 10.12, S. 484). Diese Programme enthalten neben ihrer eigentlichen und offensichtlichen Funktion weitere schädliche Funktionen, die im Hintergrund arbeiten und durch das eigentliche Programm getarnt werden. Solche schädlichen Funktionen können z. B. gedrückte Tasten protokollieren, um Passwörter auszuspionieren.

2.5.5 Autorisierungsverletzung

Dienste oder Ressourcen werden von einer Instanz genutzt, die dazu nicht berechtigt ist. Dies ist beispielsweise der Fall, wenn sich ein Benutzer eines Mehrbenutzersystems unberechtigterweise Systemadministratorprivilegien beschafft, um auf sämtliche Daten und Dienste des Systems zugreifen zu können.