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.