CAPÍTULO 1

Visão geral

OBJETIVOS DE APRENDIZADO

Depois de estudar este capítulo, você deverá ser capaz de:

- Descrever os requisitos de segurança fundamentais de confidencialidade, integridade e disponibilidade.
- Discutir os tipos de ameaças e ataques à segurança que devemos tratar e dar exemplos dos tipos de ameaças e ataques que se aplicam a diferentes categorias de ativos computacionais e de rede.
- Resumir os requisitos funcionais para a segurança de computadores.
- Descrever a arquitetura de segurança X.800 para o modelo OSI.
- Discutir as principais tendências relativas a ameaças e contramedidas.
- Entender os aspectos principais de uma estratégia de segurança abrangente.

Este capítulo dá uma visão geral da segurança de computadores. Começamos discutindo o que queremos dizer com segurança de computadores. Essencialmente, a área de segurança de computadores trata de ativos computacionais que estão sujeitos a uma variedade de ameaças e contra as quais se tomam várias medidas para proteger tais ativos. Desse modo, a próxima seção dá uma breve visão geral das categorias de ativos computacionais que usuários e gerentes de sistemas querem preservar e proteger, e examina várias ameaças e ataques que esses ativos podem sofrer. Então, examinamos as medidas que podem ser tomadas para lidar com tais ameaças e ataques. Para tal, adotamos três pontos de vista diferentes, nas Seções 1.3 a 1.5. Em seguida tratamos de algumas tendências recentes na área de segurança de computadores e apresentamos, em termos gerais, uma estratégia de segurança de computadores.

O foco deste capítulo e, na verdade, deste livro, está em três questões fundamentais:

1. Quais ativos precisamos proteger?
2. Como esses ativos são ameaçados?
3. O que podemos fazer para suavizar essas ameaças?

1.1 CONCEITOS DE SEGURANÇA DE COMPUTADORES

Uma definição de segurança de computadores

O Computer Security Handbook ("Livro de Bolso de Segurança de Computadores") do NIST [NIST95] define a expressão *segurança de computadores* da seguinte maneira:

Segurança de computadores: A proteção oferecida a um sistema de informação automatizado para atingir os objetivos apropriados de preservação da integridade, disponibilidade e confidencialidade de ativos de sistemas de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).

Essa definição apresenta três objetivos fundamentais que constituem o coração da segurança de computadores:

- **Confidencialidade:** Esse termo abrange dois conceitos relacionados:
  - **Confidencialidade de dados**[1] Garante que informações privadas ou confidenciais não fiquem disponíveis nem sejam reveladas a indivíduos não autorizados.
  - **Privacidade:** Garante que os indivíduos controlem ou influenciem quais informações sobre eles podem ser coletadas e armazenadas, e por quem e para quem tais informações podem ser reveladas.
- **Integridade:** Esse termo abrange dois conceitos relacionados:
  - **Integridade de dados:** Garante que informações e programas sejam alterados somente de maneira especificada e autorizada.
  - **Integridade de sistemas:** Garante que um sistema desempenhe sua função pretendida de maneira incólume, livre de manipulação não autorizada do sistema, seja deliberada, seja inadvertida.
- **Disponibilidade:** Garante que os sistemas funcionem prontamente e que não haja negação de serviço a usuários autorizados.

Esses três conceitos formam o que é frequentemente denominado **tríade CID** (Figura 1.1). Os três conceitos incorporam os objetivos de segurança fundamentais para dados e informações, bem como para serviços de computação. Por exemplo, o padrão NIST denominado FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*) apresenta confidencialidade, integridade e disponibilidade como os três objetivos de segurança para informações e para sistemas de informação. O FIPS PUB 199 fornece uma caracterização útil desses três objetivos em termos de requisitos e a definição de perda de segurança relativa a cada categoria:

- **Confidencialidade:** Preservar restrições autorizadas ao acesso e revelação de informações, incluindo meios para proteger a privacidade pessoal e as informações

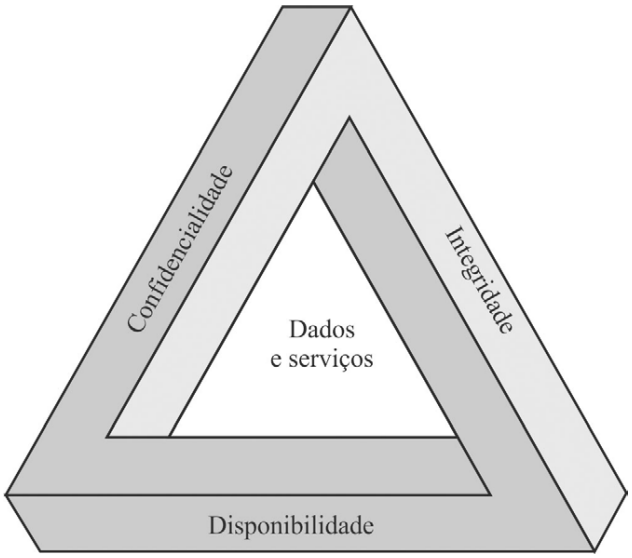

FIGURA 1.1 A tríade de requisitos de segurança

[1] A RFC 2828 define *informação* como "fatos e ideias que podem ser representados (codificados) como várias formas de dados", e *dados* como "informação em uma representação física específica, usualmente uma sequência de símbolos que têm significado; especialmente uma representação de informação que pode ser processada ou produzida por um computador". A literatura de segurança não costuma fazer grande distinção entre os dois, nem este livro.

proprietárias. Uma perda de confidencialidade consiste na revelação não autorizada de informações.

- **Integridade:** Defender contra a modificação ou destruição imprópria de informações, garantindo a irretratabilidade (ou não repúdio) e a autenticidade das informações. Uma perda de integridade consiste na modificação ou destruição não autorizada de informações.
- **Disponibilidade:** Assegurar que o acesso e o uso das informações seja confiável e realizado no tempo adequado. Uma perda de disponibilidade consiste na disrupção do acesso ou da utilização de informações ou de um sistema de informação.

Embora a utilização da tríade CID para definir objetivos de segurança seja bem estabelecida, algumas pessoas na área da segurança acreditam serem necessários conceitos adicionais para apresentar um quadro completo. Dois dos mais comumente mencionados são os seguintes:

- **Autenticidade:** A propriedade de ser genuína e poder ser verificada e confiável; confiança na validade de uma transmissão, de uma mensagem ou do originador de uma mensagem. Isso significa verificar que os usuários são quem dizem ser e que cada dado que chega ao sistema veio de uma fonte confiável.
- **Determinação de responsabilidade:** O objetivo de segurança que leva à exigência de que as ações de uma entidade sejam rastreadas e atribuídas unicamente àquela entidade. Isso dá suporte à irretratabilidade, à dissuasão, ao isolamento de falhas, à detecção e prevenção de intrusões, e à recuperação e à ação judicial após uma ação. Como sistemas verdadeiramente seguros ainda não são uma meta atingível, devemos ser capazes de rastrear uma violação de segurança até a entidade responsável. Os sistemas devem manter registros de suas atividades para permitir análise forense posterior, de modo a rastrear violações de segurança ou auxiliar em disputas sobre uma transação.

Observe que o FIPS PUB 199 inclui autenticidade como parte da integridade.

Exemplos

Agora fornecemos alguns exemplos de aplicações que ilustram os requisitos enumerados.[2] Para esses exemplos, usamos três níveis de impacto sobre organizações ou indivíduos caso haja uma quebra de segurança (isto é, uma perda de confidencialidade, integridade ou disponibilidade). Esses níveis são definidos no FIPS PUB 199:

- **Baixo:** Pode-se esperar que a perda cause efeito adverso limitado sobre operações organizacionais, ativos organizacionais ou indivíduos. Um efeito adverso limitado significa, por exemplo, que a perda de confidencialidade, integridade ou disponibilidade poderia (i) causar degradação na capacidade de completar uma tarefa até um ponto e por uma duração tal que a organização consegue executar suas funções primárias, mas a efetividade das funções sofre redução perceptível; (ii) resultar em dano desprezível a ativos organizacionais; (iii) resultar em perdas financeiras insignificantes; ou (iv) resultar em dano reduzido a indivíduos.
- **Moderado:** Pode-se esperar que a perda cause efeito adverso sério sobre operações organizacionais, ativos organizacionais ou indivíduos. Um efeito adverso sério significa, por exemplo, que a perda poderia (i) causar degradação significativa na capacidade de completar uma tarefa até um ponto e por uma duração tal que a organização consegue executar suas funções primárias, mas a efetividade das funções sofre significativa redução; (ii) resultar em dano significativo a ativos organizacionais;

[2] Esses exemplos foram retirados de um documento sobre política de segurança publicado pelo Information Technology Security and Privacy Office da Purdue University.

(iii) resultar em perda financeira significativa; ou (iv) resultar em dano significativo a indivíduos, não envolvendo perda de vida ou ferimentos sérios que ameacem a vida.

- **Alto:** Pode-se esperar que a perda cause efeito adverso grave ou catastrófico sobre operações organizacionais, ativos organizacionais ou indivíduos. Um efeito adverso grave ou catastrófico significa, por exemplo, que a perda poderia (i) causar grave degradação ou perda de capacidade de completar uma tarefa até um ponto e por uma duração tal que a organização não consegue executar uma ou mais de suas funções primárias; (ii) resultar em grande dano a ativos organizacionais; (iii) resultar em grande perda financeira; ou (iv) resultar em dano grave ou catastrófico a indivíduos, envolvendo perda de vida ou ferimentos sérios que ameacem a vida.

Confidencialidade

Informações sobre notas obtidas por estudantes em exames são um ativo cuja confidencialidade é considerada de altíssima importância pelos próprios estudantes. Nos Estados Unidos, a liberação de tais informações é regulamentada pelo Family Educational Rights and Privacy Act (FERPA). Informações sobre tais notas só podem ser disponibilizadas para estudantes, seus pais e funcionários que necessitem das informações para realizar seu serviço. Informações sobre matrículas de estudantes podem ter grau moderado de confiabilidade. Embora ainda protegidas pelo FERPA, essas informações são vistas por mais pessoas diariamente, a probabilidade de serem visadas é menor do que a de informações sobre notas de exames escolares, e sua revelação resulta em menor dano. Informações catalogadas, como listas de estudantes ou de faculdades e departamentos, podem receber uma classificação de confidencialidade baixa ou até mesmo nula. Essas informações normalmente estão disponíveis livremente ao público e são publicadas no site da escola.

Integridade

Vários aspectos de integridade são ilustrados pelo exemplo das informações de um hospital sobre as alergias de seus pacientes, armazenadas em um banco de dados. O médico tem de confiar que as informações são corretas e atualizadas. Entretanto, suponha que um funcionário (por exemplo, um enfermeiro) que está autorizado a ver e atualizar essas informações falsifique deliberadamente os dados para causar danos ao hospital. O banco de dados precisará ser restaurado rapidamente para um estado confiável e possibilitar o rastreamento e a identificação da pessoa responsável pelo erro. Informações sobre as alergias dos pacientes são um exemplo de ativo que requer alto grau de integridade. Informações inexatas poderiam resultar em sérios danos e até na morte de um paciente e expor o hospital a uma ação judicial de responsabilidade.

Um exemplo de ativo ao qual pode ser imputado um requisito de integridade de nível moderado é um site da Web que oferece um fórum para usuários registrados discutirem algum tópico específico. Um usuário registrado ou um hacker poderia falsificar algumas entradas ou desfigurar o site. Se o fórum existir para ser utilizado somente pelos usuários, se gerar pouca ou nenhuma receita de anúncios publicitários e não for usado para algo importante como pesquisas, o dano potencial não é grave. O webmaster pode sofrer alguma perda de dados, de tempo ou financeira.

Um exemplo de requisito de integridade baixa é uma votação anônima on-line. Muitos sites da Web, como empresas jornalísticas, fornecem os resultados dessas votações a seus usuários com um número muito pequeno de ressalvas. Todavia, a inexatidão e a natureza não científica dessas votações é bem entendida.

Disponibilidade

Quanto mais crítico um componente ou serviço, mais alto é o nível de disponibilidade exigido. Considere um sistema que provê serviços de autenticação para sistemas, aplicações

e dispositivos críticos. Uma interrupção do serviço resultaria na incapacidade de os clientes acessarem ativos computacionais e de funcionários acessarem os ativos de que necessitam para executar tarefas críticas. A perda do serviço traduz-se em grande perda financeira e em termos de perda de produtividade dos empregados e potencial perda de clientes.

Um exemplo do que normalmente seria classificado como ativo que requer disponibilidade moderada é um site público de uma universidade; o site provê informações sobre estudantes e doadores atuais e potenciais. Tal site não é um componente crítico do sistema de informação da universidade, mas sua indisponibilidade causará algum constrangimento.

Uma aplicação de consulta a listas telefônicas on-line seria classificada como requisito de disponibilidade baixa. Embora a perda temporária de acesso à aplicação possa ser um aborrecimento, há outros modos de acessar a informação, como uma lista em papel ou um telefonista.

Os desafios da segurança de computadores

O tema segurança de computadores é ao mesmo tempo fascinante e complexo. Algumas das razões são:

1. Segurança de computadores não é tão simples quanto poderia parecer à primeira vista ao novato. Os requisitos parecem ser simples; de fato, em sua maioria, os requisitos mais importantes para serviços de segurança podem receber rótulos autoexplicativos de uma única palavra: confidencialidade, autenticação, irretratabilidade, integridade. Mas os mecanismos usados para satisfazer esses requisitos podem ser bastante complexos, e entendê-los pode envolver raciocínio um tanto engenhoso.
2. Quando desenvolvemos determinado mecanismo ou algoritmo de segurança, devemos sempre considerar ataques potenciais a esses requisitos de segurança. Em muitos casos, ataques bem-sucedidos são projetados apenas enxergando o problema de um modo completamente diferente e, portanto, explorando uma fraqueza inesperada no mecanismo.
3. Como consequência do ponto 2, os procedimentos usados para prover determinados serviços são frequentemente anti-intuitivos. Normalmente, um mecanismo de segurança é complexo, e não fica óbvio, apenas pelo enunciado de determinado requisito, que medidas tão elaboradas são necessárias. É só quando consideramos os vários aspectos da ameaça que mecanismos de segurança elaborados fazem sentido.
4. Depois de projetados vários mecanismos de segurança, é necessário decidir onde usá-los. Isso vale tanto em termos de posicionamento físico (por exemplo, em quais pontos de uma rede certos mecanismos de segurança são necessários) quanto no sentido lógico (por exemplo, em qual camada ou camadas de uma arquitetura como a TCP/IP [Transmission Control Protocol/Internet Protocol] os mecanismos devem ser colocados).
5. Mecanismos de segurança normalmente envolvem mais de um algoritmo ou protocolo em particular. Além disso, eles exigem que os participantes estejam de posse de alguma informação secreta (por exemplo, uma chave criptográfica), o que levanta questões sobre geração, distribuição e proteção dessa informação secreta. Pode haver também uma dependência de protocolos de comunicações cujo comportamento complique a tarefa de desenvolver o mecanismo de segurança. Por exemplo, se o funcionamento adequado do mecanismo de segurança exigir que sejam fixados limites de tempo para o intervalo de trânsito de uma mensagem do remetente ao destinatário, qualquer protocolo ou rede que introduza atrasos variáveis e imprevisíveis pode fazer com que tais limites de tempo percam completamente o significado.

6. Segurança de computadores é essencialmente uma batalha de capacidade entre um perpetrador que tenta encontrar brechas e o projetista ou administrador que tenta fechá-las. A grande vantagem que o atacante tem é que só precisa descobrir uma única fraqueza, ao passo que o projetista tem de encontrar e eliminar todas as fraquezas para conseguir segurança perfeita.
7. Há uma tendência natural da parte de usuários e gerentes de sistemas de perceberem pouco benefício em fazer investimento em segurança até ocorrer uma falha de segurança.
8. Segurança requer monitoramento regular, até constante, e isso é difícil no ambiente de curto prazo e sobrecarregado de hoje.
9. Segurança ainda é muito frequentemente mero acessório a ser incorporado a um sistema depois de concluído o projeto, em vez de ser parte integral do processo de construir o projeto.
10. Muitos usuários e até mesmo administradores de segurança consideram que segurança forte atrapalha a operação eficiente e amigável ao usuário de um sistema de informação ou a utilização da informação.

As dificuldades que acabamos de enumerar serão encontradas de diversas maneiras à medida que examinarmos as várias ameaças e mecanismos de segurança neste livro.

Um modelo para segurança de computadores

Apresentamos agora um pouco de terminologia que será útil em todo o livro, baseada no RFC 2828, *Internet Security Glossary.*[3] A Tabela 1.1 define termos e a Figura 1.2 [CCPS09a] mostra a relação entre alguns desses termos. Começamos com o conceito de **recurso de sistema**, ou **ativo de sistema**, que usuários e proprietários querem proteger. Os ativos de um sistema de computador podem ser categorizados como segue:

- **Hardware:** Inclui sistemas de computador e outros dispositivos de processamento de dados, armazenamento de dados e comunicações de dados.
- **Software:** Inclui o sistema operacional, utilitários de sistema e aplicações.
- **Dados:** Incluem arquivos e bancos de dados, bem como dados relacionados à segurança, como arquivos de senhas.
- **Instalações e redes de comunicações:** Enlaces de comunicação, pontes, roteadores, e assim por diante, de redes locais e de longa distância.

No contexto da segurança, nossa preocupação é com as **vulnerabilidades** dos ativos do sistema. [NRC02] apresenta uma lista das seguintes categorias gerais de vulnerabilidades de um ativo de sistema de computador ou rede:

- Ele pode ser **corrompido,** de modo a operar de forma errônea ou dar respostas erradas. Por exemplo, valores de dados armazenados podem ser diferentes do que deveriam ser porque foram modificados inadequadamente.
- Ele pode estar **vazando**. Por exemplo, alguém que não deveria ter acesso a algumas ou a todas as informações disponíveis por meio da rede obtém tal acesso.
- Ele pode tornar-se **indisponível** ou muito lento. Isto é, usar o sistema ou rede torna-se impossível ou impraticável.

Esses três tipos gerais de vulnerabilidade correspondem aos conceitos de integridade, confidencialidade e disponibilidade, enumerados anteriormente nesta seção.

Correspondendo aos vários tipos de vulnerabilidades de um ativo de sistema estão as **ameaças** capazes de explorar essas vulnerabilidades. Uma ameaça representa um potencial dano à segurança de um ativo. Um **ataque** é uma ameaça que é executada (ação de ameaça)

[3] Consulte o Capítulo 0 se quiser uma explanação sobre RFCs.

Tabela 1.1 Terminologia de segurança de computadores
Adversário (agente fonte de ameaça)
Entidade que ataca um sistema ou é uma ameaça para ele.
Ameaça
Um potencial para violação de segurança, que existe quando há circunstância, capacidade, ação ou evento que poderia infringir a segurança e causar dano. Isto é, uma ameaça é um perigo possível que poderia explorar uma vulnerabilidade.
Ataque
Tentativa de violação da segurança do sistema que deriva de ameaça inteligente, isto é, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de envolver um método ou técnica) para burlar serviços de segurança e violar a política de segurança de um sistema.
Contramedida
Ação, dispositivo, procedimento ou técnica que reduz uma ameaça, uma vulnerabilidade ou um ataque, eliminando-o ou prevenindo-o, minimizando o dano que ele pode causar ou descobrindo-o e relatando-o de modo a possibilitar uma ação corretiva.
Política de segurança
Conjunto de regras e práticas que especificam ou regulamentam como um sistema ou organização provê serviços de segurança para proteger ativos sensíveis e críticos de um sistema.
Recurso de sistema (ativo)
Dados contidos em um sistema de informação; serviço provido por um sistema; capacidade do sistema, como poder de processamento ou largura de banda de comunicação; item de equipamento do sistema (isto é, um componente do sistema — hardware, firmware, software ou documentação); instalação que abrigue operações e equipamentos de sistema.
Risco
Expectativa de perda de segurança expressa como a probabilidade de que uma ameaça particular explorará uma vulnerabilidade particular com resultado danoso particular.
Vulnerabilidade
Falha, defeito ou fraqueza no projeto, implementação ou operação e gerenciamento de um sistema que poderia ser explorada para violar a política de segurança do sistema.
Fonte: *RFC 2828, Internet Security Glossary, maio de 2000.*

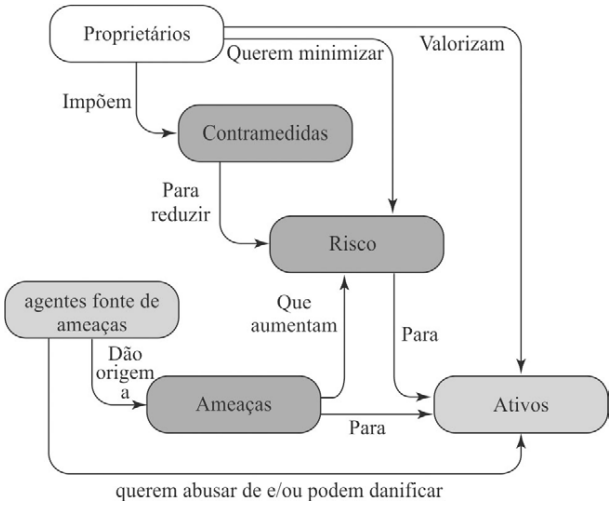

FIGURA 1.2 Conceitos e relações de segurança.

e, se bem-sucedido, resulta em uma violação indesejável de segurança ou consequência da ameaça. O agente que executa o ataque é denominado atacante ou **agente fonte de ameaça**. Podemos distinguir dois tipos de ataques:

- **Ataque ativo:** Tentativa de alterar ativos de sistemas ou afetar sua operação.
- **Ataque passivo:** Tentativa de descobrir ou fazer uso de informações advindas do sistema que não afeta ativos do sistema.

Também podemos classificar os ataques com base na sua origem:

- **Ataque interno:** Iniciado por uma entidade que está dentro do perímetro de segurança (um "usuário interno legítimo" ou "*insider*"). O *insider* está autorizado a acessar ativos de sistema, mas os usa de modo não aprovado por quem concedeu a autorização.
- **Ataque externo:** Iniciado de fora do perímetro por um usuário não autorizado ou ilegítimo do sistema (um "*outsider*"). Na Internet, atacantes externos potenciais vão de amadores curiosos a criminosos organizados, terroristas internacionais e governos hostis.

Finalmente, uma **contramedida** é qualquer meio utilizado para lidar com um ataque à segurança. O ideal seria que uma contramedida pudesse ser projetada para **impedir** o sucesso de um tipo de ataque em particular. Quando a prevenção não é possível ou falha em alguma instância, a meta é **detectar** o ataque e **recuperar** o sistema dos efeitos do ataque. Uma contramedida pode em si introduzir novas vulnerabilidades. Seja qual for o caso, é possível que vulnerabilidades residuais permaneçam após a aplicação de contramedidas. Tais vulnerabilidades podem ser exploradas por agentes fonte de ameaça que representam um nível residual de **risco** para os ativos. Os proprietários procurarão minimizar tal risco dadas outras restrições.

1.2 AMEAÇAS, ATAQUES E ATIVOS

Passamos agora a um exame mais detalhado de ameaças, ataques e ativos. Em primeiro lugar, examinamos os tipos de ameaças à segurança que devem ser tratados e depois damos alguns exemplos dos tipos de ameaças que se aplicam a diferentes categorias de ativos.

Ameaças e ataques

A Tabela 1.2, baseada na RFC 2828, descreve quatro tipos de consequências de ameaças e dá uma lista de tipos de ataques que resultam em cada consequência.

Revelação não autorizada é uma ameaça à confidencialidade. Os seguintes tipos de ataques podem resultar nessa consequência de ameaça:

- **Exposição:** Pode ser deliberada, como ocorre quando um agente interno (*insider*) divulga informações sensíveis, como números de cartões de crédito, a um agente externo (*outsider*). Também pode ser o resultado de um erro humano, de hardware ou de software, que resulta em uma entidade obtendo conhecimento não autorizado sobre dados sensíveis. Há numerosos exemplos disso, como a publicação acidental na Web, por uma universidade, de informações confidenciais de estudantes.
- **Interceptação:** Interceptação é um ataque comum no contexto de comunicações. Em uma rede local (LAN) compartilhada, como uma LAN sem fio ou uma rede Ethernet, qualquer dispositivo conectado à LAN pode receber uma cópia dos pacotes cujo destino pretendido era outro dispositivo. Na Internet, um hacker persistente pode obter acesso a tráfego de e-mail e outras transferências de dados.