**1.1 Conceitos de Segurança Informática**

Uma Definição de Segurança de Computador

O NIST Computer Security Handbook [NIST95] define o termo segurança do computador ridade da seguinte forma:

**Segurança Informática**: A proteção oferecida a um sistema de informação automatizado a fim de atingir os objetivos aplicáveis de preservação da integridade, disponibilidade, e confidencialidade dos recursos do sistema de informação (inclui hardware, software, firmware, informações/dados e telecomunicações). Esta definição apresenta três objetivos principais que estão no cerne da computação segurança:

• **Confidencialidade**: Este termo abrange dois conceitos relacionados: Confidencialidade Data1: Garante que informações privadas ou confidenciais sejam não disponibilizados ou divulgados a pessoas não autorizadas. Privacidade: garante que os indivíduos controlem ou influenciem quais informações relacionados a eles podem ser coletados e armazenados e por quem e para quem essas informações podem ser divulgadas.

• **Integridade**: Este termo abrange dois conceitos relacionados:

**Integridade dos dados**: Garante que as informações e os programas sejam alterados apenas em forma especificada e autorizada. **Integridade do sistema**: garante que um sistema execute sua função pretendida em uma maneira inalterada, livre de deliberada ou inadvertidamente não autorizada manipulação do sistema.

• **Disponibilidade**: garante que os sistemas funcionem prontamente e o serviço não seja negado aos usuários autorizados.

Esses três conceitos formam o que costuma ser chamado de tríade da CIA. Os três conceitos incorporam os objetivos fundamentais de segurança para dados e para informações e serviços de computação. Por exemplo, o padrão NIST FIPS 199 (Padrões para Categorização de Segurança de Informações Federais e Sistemas de Informação) listas confidencialidade, integridade e disponibilidade como os três objetivos de segurança para informações informação e para sistemas de informação. FIPS 199 fornece uma caracterização útil de esses três objetivos em termos de requisitos e a definição de uma perda de segurança em cada categoria:

• **Confidencialidade**: Preservar as restrições autorizadas no acesso à informação e divulgação, incluindo meios para proteger a privacidade pessoal e propriedade informações etárias. Perda de confidencialidade é a divulgação não autorizada de Informação.

• **Integridade**: proteção contra modificação ou destruição imprópria de informações, inclusive garantindo o não repúdio e a autenticidade das informações. Uma perda de integridade é a modificação ou destruição não autorizada de informações.

• **Disponibilidade**: garantir o acesso oportuno e confiável e o uso da informação. Uma perda de disponibilidade é a interrupção do acesso ou uso de informações ou uma sistema de informação. Embora o uso da tríade CIA para definir objetivos de segurança esteja bem estabelecido, alguns no campo da segurança acham que conceitos adicionais são necessários para apresentar uma imagem completa. Dois dos mais comumente mencionados são os seguintes:

• **Autenticidade**: A propriedade de ser genuíno e poder ser verificado e confiável; confiança na validade de uma transmissão, mensagem ou mensagem originador. Isso significa verificar se os usuários são quem dizem ser e se cada entrada que chega ao sistema vem de uma fonte confiável.

• **Responsabilidade**: O objetivo de segurança que gera a necessidade de ações de uma entidade a ser rastreada exclusivamente para essa entidade. Isso suporta o não-repúdio proteção, dissuasão, isolamento de falhas, detecção e prevenção de intrusão e pós- recuperação de ação e ação judicial. Como os sistemas verdadeiramente seguros ainda não são uma objetivo alcançável, devemos ser capazes de rastrear uma violação de segurança para um responsável desta festa. Os sistemas devem manter registros de suas atividades para permitir análises forenses posteriores, análise para rastrear violações de segurança ou para ajudar em disputas de transações.

Exemplos

Agora fornecemos alguns exemplos de aplicações que ilustram os requisitos que acabamos de enumerar.

2 Para esses exemplos, usamos três níveis de impacto nas organizações ou indivíduos caso haja uma quebra de segurança (ou seja, perda de confidencialidade, integridade ou disponibilidade). Esses níveis são definidos no FIPS PUB 199:

• Baixa: pode-se esperar que a perda tenha um efeito adverso limitado na organização operações nacionais, ativos organizacionais ou indivíduos. Um adverso limitado efeito significa que, por exemplo, a perda de confidencialidade, integridade ou disponibilidade habilidade pode (i) causar uma degradação na capacidade da missão até certo ponto e duração que a organização é capaz de desempenhar suas funções primárias, mas o a eficácia das funções é visivelmente reduzida; (ii) resultar em danos menores idade para ativos organizacionais; (iii) resultar em pequena perda financeira; ou (iv) resultar em danos menores aos indivíduos.

• Moderado: pode-se esperar que a perda tenha um efeito adverso sério sobre operações organizacionais, ativos organizacionais ou indivíduos. Um sério efeito adverso significa que, por exemplo, a perda pode (i) causar um impacto significativo degradação significativa na capacidade de missão em uma extensão e duração que o organização é capaz de desempenhar suas funções primárias, mas a eficácia das funções é significativamente reduzida; (ii) resultar em danos significativos ativos organizacionais; (iii) resultar em perdas financeiras significativas; ou (iv) resultar em dano significativo a indivíduos que não envolva perda de vida ou grave, ferimentos com risco de vida.

• Alto: Pode-se esperar que a perda tenha um efeito adverso grave ou catastrófico efeito sobre as operações organizacionais, ativos organizacionais ou indivíduos. Um efeito adverso grave ou catastrófico significa que, por exemplo, a perda pode (i) causar uma degradação severa ou perda da capacidade da missão em uma extensão e período em que a organização não é capaz de realizar um ou mais de seus funções de Maria; (ii) resultar em grandes danos aos ativos organizacionais; (iii) resultado em grande perda financeira; ou (iv) resultar em danos graves ou catastróficos para indivíduos também envolvendo a perda de vidas ou lesões graves com risco de vida.

Confidencialidade As informações das notas dos alunos são um ativo cuja confidencialidade é considerado muito importante pelos alunos. Nos Estados Unidos, o lançamento de tais informações são regulamentadas pela Lei de Privacidade e Direitos Educacionais da Família (FERPA). As informações sobre as notas devem estar disponíveis apenas para os alunos, seus pais, e funcionários que precisam das informações para realizar seu trabalho. Matrícula do aluno informações podem ter uma classificação de confidencialidade moderada. Embora ainda coberto por FERPA, esta informação é vista por mais pessoas diariamente, é menos provável que seja alvo do que informações de grau e resulta em menos dano se divulgado. Diretório informações, como listas de alunos ou professores ou listas departamentais, podem ser recebeu uma classificação de confidencialidade baixa ou mesmo nenhuma classificação. Esta informação é tipicamente disponíveis gratuitamente ao público e publicados no site da escola.

Integridade Vários aspectos da integridade são ilustrados pelo exemplo de um hospital informações de alergia do paciente armazenadas em um banco de dados. O médico deve ser capaz de confiança de que as informações são corretas e atuais. Agora suponha que um empregado (por exemplo, uma enfermeira) que está autorizada a visualizar e atualizar essas informações deliberadamente falsifica os dados para causar danos ao hospital. O banco de dados precisa ser restaurado para uma base confiável rapidamente, e deve ser possível rastrear o erro de volta a pessoa responsável. As informações de alergia do paciente são um exemplo de ativo com alto exigência de integridade. Informações imprecisas podem resultar em danos graves ou morte de um paciente e expor o hospital a responsabilidades maciças.

Um exemplo de ativo ao qual pode ser atribuído um nível moderado de integridade requisito é um site da Web que oferece um fórum para usuários registrados para discutir alguns Tópico especifico. Um usuário registrado ou um hacker pode falsificar algumas entradas ou desfigurar o site. Se o fórum existe apenas para usufruto dos usuários, traz em pouca ou nenhuma receita publicitária, e não é usado para algo importante como como pesquisa, então o dano potencial não é grave. O Web master pode experimentar alguns dados, financeiros e perda de tempo.

Um exemplo de requisito de baixa integridade é uma pesquisa on-line anônima. Muitos Sites da Web, como organizações de notícias, oferecem essas pesquisas a seus usuários com muito poucos proteções. No entanto, a imprecisão e a natureza não científica de tais pesquisas são bem entendido.

Disponibilidade Quanto mais crítico um componente ou serviço, maior é o nível de disponibilidade necessária. Considere um sistema que forneça serviços de autenticação vícios para sistemas críticos, aplicativos e dispositivos. Uma interrupção do serviço resulta na incapacidade dos clientes de acessar recursos de computação e da equipe de acessar os recursos de que precisam para realizar tarefas críticas. A perda do serviço se traduz em uma grande perda financeira na perda de produtividade e potencial dos funcionários perda de cliente.

Um exemplo de um ativo que normalmente seria classificado como tendo um impacto moderado o requisito de disponibilidade é um site público de uma universidade; o site fornece informações para alunos e doadores atuais e futuros. Tal site não é um componente crítico do sistema de informação da universidade, mas sua indisponibilidade causar algum constrangimento.

Um aplicativo de pesquisa de lista telefônica on-line seria classificado como de baixa requisito de disponibilidade. Embora a perda temporária do aplicativo possa ser um aborrecimento, existem outras maneiras de acessar as informações, como uma cópia impressa diretório ou o operador.

**Os desafios da segurança informática**

A segurança de computadores e redes é fascinante e complexa. Alguns dos seguem as razões:

1. A segurança não é tão simples quanto pode parecer para o iniciante. A exigência- mentos parecem ser diretos; de fato, a maioria dos principais requisitos para serviços de segurança podem receber rótulos autoexplicativos de uma só palavra: confidencialidade, autenticação, não-repúdio ou integridade. Mas os mecanismos usados atender a esses requisitos pode ser bastante complexo, e entendê-los pode envolver um raciocínio bastante sutil.

2. Ao desenvolver um determinado mecanismo ou algoritmo de segurança, deve-se sempre

considere possíveis ataques a esses recursos de segurança. Em muitos casos, sucessivos ataques são projetados olhando para o problema de uma maneira completamente diferente,

explorando, portanto, uma fraqueza inesperada no mecanismo.

3. Em virtude do ponto 2, os procedimentos utilizados para a prestação de determinados serviços são muitas vezes contra-intuitivo. Normalmente, um mecanismo de segurança é complexo e não é óbvio a partir da declaração de um requisito particular que tal elaboração de medidas de taxa são necessárias. Somente quando os vários aspectos da ameaça são considerados mecanismos de segurança elaborados fazem sentido.

4. Tendo desenhado vários mecanismos de segurança, é necessário decidir onde para usá-los. Isso é verdade tanto em termos de posicionamento físico (por exemplo, em que pontos em uma rede são necessários certos mecanismos de segurança) e em um sentido lógico (por exemplo, em qual camada ou camadas de uma arquitetura como TCP/IP [Transmission Protocolo de Controle/Protocolo de Internet] devem ser colocados mecanismos).

5. Mecanismos de segurança geralmente envolvem mais do que um determinado algoritmo ou protocolo. Eles também exigem que os participantes estejam de posse de algum segredo

informações (por exemplo, uma chave de criptografia), o que levanta questões sobre a criação, distribuição e proteção dessas informações secretas. Também pode ser uma dependência de protocolos de comunicação cujo comportamento pode complicar a tarefa de desenvolver o mecanismo de segurança. Por exemplo, se o correto funcionamento do mecanismo de segurança requer o estabelecimento de limites de tempo no transporte tempo de espera de uma mensagem do remetente ao destinatário, então qualquer protocolo ou rede que introduz atrasos variáveis e imprevisíveis pode tornar esses limites de tempo

sem significado.

6. A segurança de computadores e redes é essencialmente uma batalha de inteligência entre um penetrador que tenta encontrar buracos e o designer ou administrador que tenta fechá-los. A grande vantagem que o atacante tem é que ele precisa encontrar apenas uma única fraqueza, enquanto o designer deve encontrar e eliminar todos pontos fracos para alcançar a segurança perfeita.

7. Existe uma tendência natural por parte dos usuários e gerentes do sistema de realizar recebem pouco benefício do investimento em segurança até que ocorra uma falha de segurança.

8. A segurança requer monitoramento regular, mesmo constante, e isso é difícil em ambiente sobrecarregado de curto prazo de hoje.

9. A segurança ainda é muitas vezes uma reflexão tardia para ser incorporada a um sistema após a conclusão do projeto, em vez de ser parte integrante do projeto processo.

10. Muitos usuários e até mesmo administradores de segurança veem uma segurança forte como um impedimento para a operação eficiente e amigável de um sistema de informação ou uso de Informação.

As dificuldades que acabamos de enumerar serão encontradas de várias maneiras à medida que examine as várias ameaças e mecanismos de segurança ao longo deste livro.