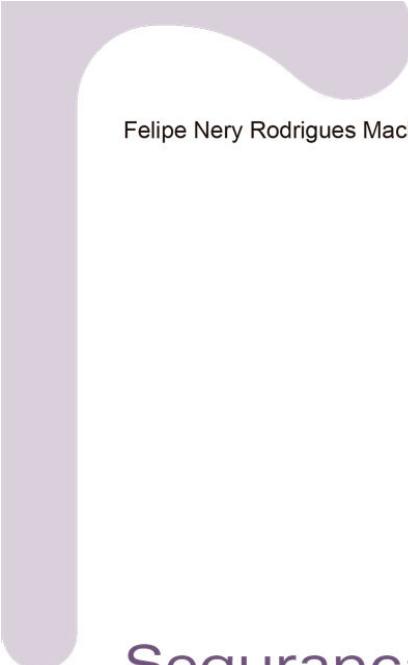


SEGURANÇA DA INFORMAÇÃO

Princípios e Controle de Ameaças

érica





Felipe Nery Rodrigues Machado

Segurança da Informação

Princípios e Controle de Ameaças

1^a Edição



Saraiva



saraiva
EDUCAÇÃO

Érica

Av. das Nações Unidas, 7221, 1º Andar, Setor B
Pinheiros – São Paulo – SP – CEP: 05425-902
PABX (11) 3613-3000

SAC

0800-0117875

De 2ª a 6ª, das 8h30 às 19h30

www.editorasaraiva.com.br/contato

Diretoria executiva Flávia Alves Bravin

Diretora editorial Renata Pascual Müller

Gerência editorial Rita de Cássia S. Puoço

Editora de aquisições Rosana Ap. Alves dos Santos

Editoras Paula Hercy Cardoso Craveiro
Silvia Campos Ferreira

Assistente editorial Rafael Henrique Lima Fulanetti

Produtoras editoriais Camilla Felix Cianelli Chaves
Laudemir Marinho dos Santos

Serviços editoriais Juliana Bojczuk Fermino
Kelli Priscila Pinto
Marília Cordeiro

Revisão Édio Pullig

Projeto gráfico e Diagramação MKX Editorial

Adaptação para eBook Cinthia Guedes

ISBN 978-85-365-0950-1

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
ANGÉLICA ILACQUA CRB-8/7057

Machado, Felipe Nery Rodrigues

Segurança da Informação: princípios e controle de ameaças / Felipe Nery Rodrigues Machado. -- 1. ed. -- São Paulo: Érica, 2014.

Bibliografia

ISBN 978-85-365-0950-1

1. Internet - Medidas de segurança 2. Redes de computadores - Medidas de segurança 3. Segurança de computadores I. Título.

CDD 005.8

Índices para catálogo sistemático:

1. Dados: Segurança: Computadores 005.8
2. Segurança dos dados: Computadores 005.8

Copyright© 2019 Saraiva Educação

Todos os direitos reservados.

1^a edição

Nenhuma parte desta publicação poderá ser reproduzida por qualquer meio ou forma sem a prévia autorização da Editora Saraiva. A violação dos direitos autorais é crime estabelecido na lei nº 9.610/98 e punido pelo artigo 184 do Código Penal.

CL 642430

Agradecimento

À minha esposa Maria Cristina Machado, pela constante luta por uma qualidade de vida melhor para toda nossa família, pela busca da paz entre todas as pessoas, pelo carinho e amor que me dá e por ser antes de tudo um exemplo de ser humano.

Ao meu filho Samir, pelo auxílio na adequação de linguagem técnica para jovens estudantes de ensino médio.

Ao meu enteado João Pedro, pela revisão e leitura para comprovação do entendimento da linguagem aplicada a esta obra, com sua visão e espírito de estudante de nível médio.

Aos amigos Fabrício Beltrami da Silva e Jorge Nitschke, pelo apoio e materiais cedidos para a elaboração deste livro.

Sobre o autor

Felipe Nery Rodrigues Machado , consultor há mais de trinta anos na área de desenvolvimento de sistemas, atua como analista de sistemas e de negócios. Com formação em engenharia mecânica, possui vasta experiência na elaboração de projetos de sistemas para banco de dados e profundos conhecimentos em metodologias de desenvolvimento, modelagem e implementação de processos de negócio financeiro, industrial e em logística, entre outras verticais de negócio, com utilização de sistemas automatizados, processos, frameworks e modelagem de dados.

Especialista em projetos de bancos de dados para aplicações transacionais e gerenciais, com vasta experiência no desenvolvimento de projetos de bancos de dados para as mais diversas áreas de negócio, tais como indústria metalúrgica, indústria de alimentos, varejo e atacado, jornais e televisão, distribuição de produtos, logística, concessionárias de automóveis, órgãos públicos diversos, hospitais e companhias aéreas.

Sua experiência abrange o ciclo completo de negócios de uma organização, tendo já desenvolvido igualmente aplicações com arquitetura de Data Warehouse, processos de ETL, com grande ênfase em modelagem multidimensional e arquitetura de processos OLAP.

Foi professor universitário de disciplinas de bancos de dados e metodologias de desenvolvimento e de pós-graduação em gerência de projetos de sistemas no Rio de Janeiro. Dedica-se à pesquisa e divulgação das técnicas e metodologias do estado da arte em

desenvolvimento de aplicações. É pesquisador de todos os temas que envolvem projeto e implantação e utilização de sistemas de informação.

Autor dos livros *Tecnologia e projeto de Data Warehouse*, *Banco de dados: projeto e implementação*, *Projeto de banco de dados – uma visão prática* e *Gestão e análise de requisitos de software*, todos publicados pela Editora Érica e adotados nas principais universidades e cursos técnicos de informática do país e em Portugal.

Sumário

Agradecimento

Sobre o autor

Apresentação

A importância do aprendizado da segurança da informação

Capítulo 1 – Por que Segurança da Informação

1.1 Conceitos gerais

1.2 Princípios fundamentais de segurança

Confidencialidade

Integridade

Disponibilidade

1.3 Informação

1.4 Sistema de informação

1.5 O que são bancos de dados

1.6 Log

1.7 Sociedade e segurança da informação

1.7.1 Notícias de segurança da informação

1.7.2 As tendências em segurança

1.7.3 Mais notícias para você

Capítulo 2 – Redes e Internet

2.1 Acesso a uma rede

2.2 O que são redes de computadores

2.2.1 Objetivos de uma rede

2.2.2 Protocolos de comunicação de redes

2.2.3 Endereço IP

2.2.3.1 Hosts

2.2.4 DNS – Domain Name System

2.2.5 Como funciona uma conexão à internet

2.2.5.1 Backbones

2.2.5.2 Pacotes de dados

2.2.5.3 Conectando à Internet

Capítulo 3 – Princípios da Segurança da Informação

3.1 Princípio da integridade de informação

3.2 Princípio da confidencialidade de informação

3.2.1 Engenharia social

3.2.2 Grau de confidencialidade

3.3 Princípio da disponibilidade de informação

3.3.1 Vulnerabilidades

3.4 Políticas de segurança

3.4.1 Normas

3.4.2 Linhas recomendadas (baselines)

3.4.3 Diretrizes

3.4.4 Procedimentos

Capítulo 4 – As Ameaças à Segurança da Informação

4.1 Introdução

4.2 Ameaças

4.2.1 Ameaças fundamentais

4.2.1.1 Vazamento de informações

4.2.1.2 Violação de integridade

4.2.1.3 Indisponibilidade de serviços de informática

4.2.1.4 Acesso e uso não autorizado

4.2.2 Outros tipos de ameaças

4.2.2.1 Mascaramento

4.2.2.2 Desvio de controles (bypass)

4.2.2.3 Violação autorizada

4.2.2.4 Ameaças programadas

4.3 O que são vírus, worms (vermes) e trojans (cavalos de troia)

4.3.1 Vírus

4.3.2 O que é um trojan (cavalo de troia)?

4.3.3 O que é um worm?

4.4 Tipos de vírus

4.4.1 Vírus de infecção de arquivo

4.4.2 Vírus de setor de inicialização (vírus de boot)

4.4.3 Vírus do registro mestre de inicialização

- 4.4.4 Vírus múltiplos
- 4.4.5 Vírus de macro
- 4.4.6 Síntese sobre vírus na visão de um fabricante de antivírus
- 4.5 Worms
 - 4.5.1 Propagação de worms
 - 4.5.1.1 Identificação dos computadores-alvo
 - 4.5.1.2 Envio das cópias
 - 4.5.1.3 Ativação das cópias
- 4.4.7.4 Reinício do processo
- 4.6 O que são spywares
 - 4.6.1 Tipos de spywares
 - 4.6.1.1 Keylogger
 - 4.6.1.2 Screenlogger
 - 4.6.1.3 Adware
- 4.7 Backdoor
 - 4.7.1 Consequências de um backdoor

Capítulo 5 – Controle de Acessos

- 5.1 Introdução
- 5.2 Controle de acessos
 - 5.2.1 Identificação
 - 5.2.1.1 Scanner de retina
 - 5.2.1.2 Scanner de íris
 - 5.2.2 Autenticação
 - 5.2.2.1 Passwords
 - 5.2.2.2 Dispositivo de token
 - 5.2.3 Outros métodos de autenticação
 - 5.2.3.1 Chaves criptografadas
 - 5.2.3.2 Password de frase (passphrase)
 - 5.2.3.3 Cartões de memória
 - 5.2.3.4 Cartões inteligentes (smart cards)
- 5.3 Monitoramento de controle de acesso

Capítulo 6 – Firewalls e Detecção de Intrusão

- 6.1 Introdução
- 6.2 A utilização de acesso à internet em redes corporativas
- 6.3 O que é um firewall?

- 6.3.1 Como um firewall funciona?
- 6.3.2 Tipos de firewall – Firewall em forma de softwares
 - 6.3.2.1 Filtragem de pacotes (packet filtering)
 - 6.3.2.2 Filtragens estática e dinâmica
 - 6.3.2.3 Firewall de aplicação ou proxy de serviços (Proxy)
 - 6.3.2.4 Inspeção de estados (stateful inspection)
 - 6.3.2.5 Firewalls pessoais
 - 6.3.2.6 Firewalls de conteúdo
 - 6.3.2.7 Firewall de hardware
- 6.3.3 Limitações dos firewalls
 - 6.3.3.1 Políticas de segurança para firewalls
- 6.4 Sistemas de detecção de intrusão
 - 6.4.1 Mas o que são intrusos?
 - 6.4.2 Tipos de sistemas de detecção de intrusão

Capítulo 7 – Antivírus

- 7.1 O que é software antivírus?
- 7.2 Como funciona?
 - 7.2.1 Análise heurística
 - 7.2.2 Arquivos em quarentena
 - 7.2.3 Falso positivo e falso negativo
 - 7.2.4 Arquivos executáveis
 - 7.2.5 Assinaturas de vírus
 - 7.2.6 Síntese das funções dos programas antivírus
 - 7.2.7 A importância do antivírus

Capítulo 8 – Segurança em Dispositivos Móveis

- 8.1 Introdução
- 8.2 Utilização de dispositivos móveis
 - 8.2.1 Smartphones e códigos maliciosos
 - 8.2.2 Tablets e códigos maliciosos
 - 8.2.3 Segurança em tablets
 - 8.2.4 Segurança em conexões WI-FI
 - 8.2.5 Acessando remotamente uma Rede com Tablets
 - 8.2.6 Conclusão sobre redes sem fio

Capítulo 9 – Controles e Processos de Segurança

- 9.1 Introdução
- 9.2 Classificação de dados
- 9.3 Backups – cópias de segurança
 - 9.3.1 Políticas de backup
 - 9.3.2 Tipos de backup
 - 9.3.2.1 Backup geral de cópia
 - 9.3.2.2 Backup diário
 - 9.3.2.3 Backup incremental
 - 9.3.2.4 Backup normal
 - 9.4 A utilização de mídias removíveis

Capítulo 10 – Criptografia e Certificação Digital

- 10.1 Criptografia
 - 10.1.1 Criptografia simétrica
 - 10.1.2 Criptografia assimétrica
- 10.2 Certificação digital
 - 10.2.1 Função hash
 - 10.2.2 Assinatura digital
 - 10.2.3 Certificado digital
 - 10.2.4 Política de e-mail
 - 10.2.4.1 Aspectos legais
 - 10.2.4.2 Aspectos éticos de e-mail

Capítulo 11 – Segurança Física

- 11.1 Introdução
- 11.2 Segurança do ambiente

Bibliografia

Marcas Registradas

Apresentação

A importância do aprendizado da segurança da informação

Vivemos na “Era da Conectividade”, em que a citação do filósofo francês René Descartes “*penso, logo existo*” poderia ser reformulada para “*estou conectado, logo existo*”. Uma era em que não ter um endereço de e-mail, não navegar na internet ou não acessar ou estar em redes sociais, deixa você excluído da sociedade e nos faz perder oportunidades, sem informações ficamos desatualizados e perdemos muito da comunicação com amigos, familiares e empresas, ou seja, fora deste mundo chamado virtual e em consequência do que acontece no mundo como um todo, seja local, da empresa, das notícias e do que acontece em qualquer lugar agora, ontem ou no passado mais longínquo.

Vivemos em função de informações, sejam em papel ou virtuais, que de alguma forma se localizam nos bancos de dados de uma empresa ou no seu próprio computador pessoal.

Mas estas informações são voláteis e frágeis, muito frágeis.

Hoje, elas podem desaparecer mais rápido que um piscar de olhos, um impulso elétrico, em velocidades cada dia maiores com o aumento das chamadas bandas largas de internet.

Atualmente a posse e o uso do conhecimento passaram a ser um fator estratégico decisivo para muitas empresas, corporações e pessoas, inclusive para você, leitor.

Estas informações estão constantemente expostas a diversos tipos de ameaças, que podem representar prejuízos incalculáveis.

As vulnerabilidades e fragilidades em sistemas de informação pessoais ou de empresas podem causar problemas graves a um negócio, ou até a nossa vida pessoal. Por isso é muito importante compreender os conceitos necessários para combatê-las e, assim, nos defendermos de possíveis ataques às informações pessoais ou empresariais.

Todos os dias centenas de sistemas vitais são interconectados, operando em conjunto com outros sistemas e tornando a vida das pessoas cada dia mais fácil – e perigosa!

São sistemas de controle médico: máquinas de vigilância de pacientes, diagnósticos pela rede e até cirurgias online; sistemas de controle aéreo: interoperabilidade entre diversos aeroportos; sistemas de trânsito: semáforos, pontes móveis, pedágios.

Até sistemas de monitoramento de vulcões e meteorológicos enviam seus alarmes e avisos por alguma rede, alcançando dimensões mundiais – sem contar ainda com compras e vendas pela internet, pagamentos online com segurança, internet banking, entre outras.

Testemunhamos, no ano de 2013, as polêmicas denúncias de Edward Snowden, diretamente relacionadas à segurança da informação e ao acesso de informações e dados de pessoas, empresas e órgãos governamentais. Controles foram burlados, ou aproveitando a ausência destes controles, para obtenção de informações privilegiadas para os mais diversos fins.

Todos os dias temos notícias de ataques de hackers, invasões de sites, roubo de senhas e dados de clientes de bancos, lojas ou organizações.

Torna-se necessário a cada dia capacitar um número maior de profissionais nos conceitos e boas práticas em segurança da informação e, assim, fazer com que os processos necessários para

a redução dos riscos e a proteção dos ativos sejam criados e que a cultura de segurança se espalhe cada vez mais pelas empresas.

Hoje as principais empresas do mercado online (compras via web) oferecem plataformas seguras de troca de dados privados e também estabelecem políticas bem claras para segurança da informação, no que diz respeito ao compartilhamento de dados e ao não rastreamento de usuários.

Entretanto, não sabemos se isso é o suficiente: **Privacidade** é um assunto muito sério e isso deve ser levado em consideração.

Após o caso Snowden, ficou mais complicado, porque as pessoas em geral perceberam o tamanho e a gravidade do problema.

Por seu caráter abrangente, o livro pode ser também utilizado como apoio em disciplinas de cursos de graduação e lido por analistas de sistemas iniciantes.

Os conceitos apresentados com certeza auxiliam os profissionais na realização de suas tarefas com qualidade.

Finalmente, cabe um alerta a você, estudante: a proposta deste livro não é apresentar uma receita de bolo a ser aplicada em seus projetos para obtenção de sucesso rápido e seguro, muito menos que todas as questões abordadas venham a ser incorporadas indiscriminadamente. Mas sim ajudá-lo a compreender e dominar de forma sucinta os conceitos e as boas práticas em segurança da informação.

O autor

1

Por que Segurança da Informação

Para começar

Este capítulo tem como proposta apresentar os conceitos básicos da segurança da informação.

Em uma linguagem bastante simples e didática, detalhamos algumas ameaças e buscamos mostrar como estas ameaças interagem conosco e como podemos melhorar a segurança de informações da sociedade. As informações apresentadas formam a base necessária para entender tudo o que envolve o assunto, bem como suas definições e modos de uso. Assim compreenderemos de maneira simples o que parece ser de alta complexidade e estaremos mais bem preparados para as oportunidades do mercado de trabalho ou para continuarmos estudando sobre o assunto.

1.1 Conceitos gerais

Você já deve ter ouvido falar em vírus que causam prejuízos de milhões de dólares, hackers que capturam informações de cartões de crédito de instituições financeiras e sites de grandes empresas que foram atacados e tiveram seu acesso interrompido por razões políticas. Já deve ter ouvido falar também em informações secretas de governos, ou empresas, que foram divulgadas por hackers.

De certa maneira, essas situações podem parecer os principais problemas enfrentados pela segurança da informação. Contudo, tais atividades não são as únicas preocupações de uma empresa, ou de um profissional de segurança, no que diz respeito às tarefas diárias ou mensais de segurança.

Embora os vírus e os hackers apareçam em muitas manchetes de jornais, o gerenciamento de segurança é, dentro do núcleo de informática, o responsável pela segurança da informação de uma empresa, e mesmo não aparecendo nas manchetes dedicam-se a evitar os ataques como os noticiados na mídia.

O gerenciamento de segurança inclui a gestão de riscos, as políticas de segurança e a educação de segurança de todos os funcionários. São estes três componentes principais que servem como base do programa de segurança de qualquer empresa.

O universo da gestão de segurança da informação envolve determinação de objetivos, escopo, políticas, prioridades, padrões e estratégias.

Os objetivos da segurança da informação baseiam-se na identificação adequada dos ativos de informação de uma empresa, atribuindo valores para estes ativos, desenvolvimento,

documentação e implementação de políticas de segurança, procedimentos, normas e diretrizes, que devem fornecer integridade, confidencialidade e disponibilidade da informação.

1.2 Princípios fundamentais de segurança

Existem vários objetivos, uns pequenos e outros grandes, em um programa de segurança. Mas os três princípios centrais em todo e qualquer programa de segurança da informação são: *confidencialidade, integridade e disponibilidade*, também conhecidos como a tríade CIA.

Confidencialidade

Confidencialidade é a capacidade de garantir que o nível necessário de sigilo seja aplicado em cada junção de dados em processamento. Além disso, trata-se da prevenção contra a divulgação não autorizada dos mesmos.

Os atacantes podem burlar os mecanismos de confidencialidade por meio de monitoramento de rede (chamado surf de ombro¹), engenharia social, e roubar arquivos de senhas.

A confidencialidade pode ser fornecida por meio de técnicas de criptografia de dados e da forma como eles são armazenados e transmitidos, assim como por meio de acompanhamento de tráfego de rede, controle de acesso rigoroso, classificação de dados e treinamento de pessoal sobre os procedimentos adequados na utilização de informações na empresa.

Integridade

A integridade é a garantia de rigor e confiabilidade das informações e sistemas e de que não ocorrerão modificações não autorizadas de dados.

Os mecanismos de hardware, software e comunicação devem trabalhar de maneira conjunta para manter e processar dados corretamente e movimentar dados para os destinos desejados sem qualquer alteração não autorizada ou não esperada.

Os sistemas da empresa e a rede devem ser protegidos contra interferências e contaminações externas ao seu ambiente tecnológico.

Disponibilidade

É a capacidade que os sistemas e as redes devem ter para executar e disponibilizar os dados de forma previsível e adequada às necessidades da empresa.

Eles devem estar aptos a recuperar quedas de disponibilidade de forma rápida e segura e a garantir que a produtividade das operações da empresa não seja afetada significativamente.

A disponibilidade de sistemas pode ser afetada por falhas de equipamentos ou de softwares.

Backups, também conhecidos como cópias de segurança, devem estar disponíveis para uma rápida recuperação de sistemas e dados críticos na empresa.

Aspectos ambientais como calor, frio, umidade, eletricidade estática e produtos contaminantes podem afetar a disponibilidade de sistemas e dados.

Como veremos a seguir, os ataques de negação de serviços (DoS) são os mais populares métodos que hackers utilizam para perturbar e afetar a disponibilidade de informações e sistemas e, consequentemente, a produtividade destes sistemas. Estes ataques são feitos para reduzir ou bloquear o acesso de usuários a recursos de sistemas e informações, normalmente em sites de grandes e médias empresas.

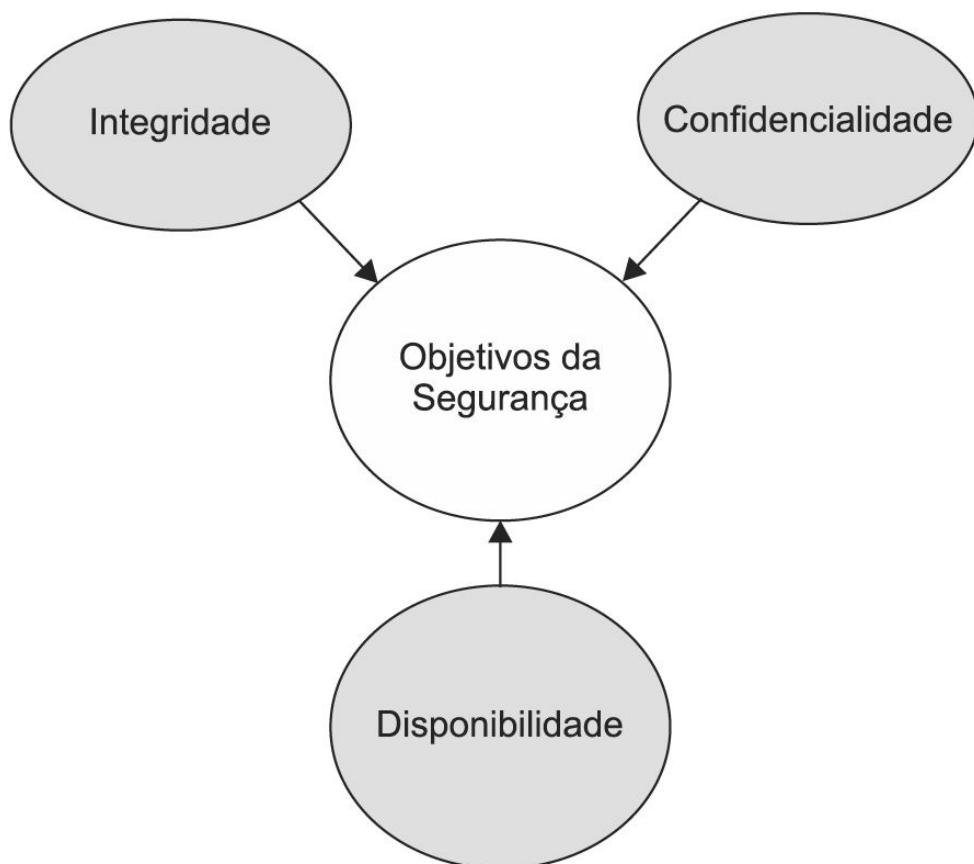


Figura 1.1 – CIA, a tríade de segurança.

A seguir falaremos sobre os principais conceitos da segurança da informação e por que ela é tão importante para os negócios de uma empresa e para você. Antes disso, porém, temos de conhecer alguns conceitos da área de tecnologia da informação, que são fundamentais para entendê-los corretamente.

Nosso objetivo, aqui, é mostrar a você, leitor, como conseguir um ambiente seguro para a informação.

1.3 Informação

O que é informação?

Ao longo dos anos de experiência no desenvolvimento de sistemas de informação, observamos que existe uma grande dificuldade das pessoas em geral para entenderem a diferença entre *informação e dados*.

A *informação* acrescenta algo ao conhecimento de uma realidade analisada. Por exemplo, a dosagem que um paciente precisa receber de um determinado remédio é uma *informação*.

O *dado* é uma representação, um registro de uma informação.

Esse *dado* pode ser registrado fisicamente em um papel (receita médica), em um disco de computador ou através de um impulso elétrico etc.

Esse registro pode ser o gerador de uma série de processos que influenciam a realidade observada (salvar a vida de um paciente, tocar um alarme etc.).

O tratamento das informações dá origem a vários tipos de *dados*, porém o *dado* deve registrar apenas os aspectos realmente relevantes da *informação*. Ou seja, o endereço do fabricante do remédio, por exemplo, não tem qualquer interesse para um sistema de controle que mantém a vida dos pacientes em um CTI.

Podemos concluir, então, que em um sistema de informações estão todas as informações necessárias ao objetivo do sistema (manter a vida do paciente).

Os *dados* originados dessas informações serão processados pelo que denomina *sistema de informações*.

Porém, por definição, os computadores não processam informações, mas sim *dados*.

Informação	Dado
Hoje está muito quente.	Temperatura atual de 38 °C.

1.4 Sistema de informação

Um sistema de informação é em princípio a automação de todos os processos manuais sobre os dados de uma determinada área ou empresa.

Um *sistema de informações* é baseado na premissa apresentada graficamente na Figura 1.2.

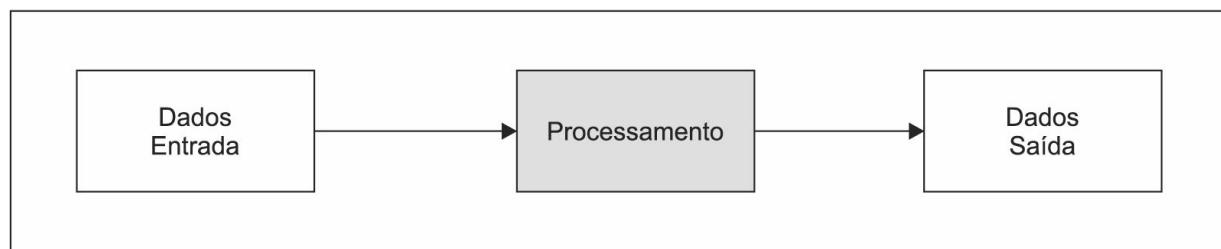


Figura 1.2 – Sistema de informações.

Então, tudo que compõe as caixinhas do desenho, na realidade, faz parte de um *sistema de informações*:

- » O que entra (por exemplo, dados, informações, eventos, entre outros) é um requisito;
- » Para que seja executado, o processamento a ser realizado tem regras, fórmulas, normas, critérios, arquivos, tabelas etc., que compõem os chamados requisitos funcionais de sistemas de informação;
- » A saída desse processamento também é composta de dados e informações, ou de disparo de eventos.

Um sistema de informação deve ser considerado sempre como um composto de um componente social e de um conjunto de dados e processamentos automatizados destes dados por meio de tecnologias computacionais.

O componente social inclui pessoas, processos, tarefas, informações e documentos. O segundo componente consiste nos meios tecnológicos (máquinas, computadores, redes de comunicação, linguagens de programação, telas de interfaces) que se interligam com o chamado componente social.

As pessoas e os processos que rotineiramente executam, e também os dados e documentos que criam, alteram, apagam e consultam, fazem parte do sistema de informações, compondo algo maior que simplesmente um software. Afinal, além de possuir o hardware e o software, também possui e realiza os processos que dependem de atividades e tarefas que são muitas vezes executadas fora dos computadores por pessoas.

A importância do conjunto social reside no fato de que os sistemas de informação, para ter a eficácia desejada, dependem diretamente da interação das pessoas que os criam e desenvolvem, de quem os acessa e utiliza. Eles não nascem do nada, não fazem nada sem a interferência humana.

Uma das preocupações da segurança da informação é proteger os elementos que compõem a informação e seus meios de comunicação e manipulação.

Sistemas de informação são também utilizados em empresas para dar apoio à tomada de decisões, atuando, além do processamento das transações rotineiras de negócio, também no planejamento e no controle operacional, no planejamento gerencial. E, finalmente, servem de base para as estratégias e políticas de uma empresa.

Lembre-se

“Informação é o resultado do tratamento dos dados existentes acerca de alguém ou de alguma coisa.”

1.5 O que são bancos de dados

Um banco de dados pode ser definido como um conjunto de dados devidamente relacionados.

Podemos compreender como dados os objetos que podem ser armazenados e que possuem um significado implícito. Porém o significado do termo banco de dados é mais restrito.

Um banco de dados possui as seguintes propriedades:

- » É uma coleção lógica coerente de dados com um significado inerente; uma disposição desordenada dos dados não pode ser referenciada como banco de dados.
- » Ele é projetado, construído e preenchido com valores de dados para um propósito específico; um banco de dados possui um conjunto predefinido de usuários e de aplicações.
- » Ele representa algum aspecto do mundo real, chamado de minimundo; qualquer alteração efetuada no minimundo é automaticamente refletida no banco de dados.

Antes somente era considerado banco de dados uma coleção lógica coerente de dados com um significado inerente e disposta de forma ordenada. Uma disposição desordenada de dados, por sua vez, não era considerada um banco de dados.

Hoje, entretanto, dados não estruturados e até mesmo desordenados são considerados banco de dados, pois caracterizam o que se denomina dados não estruturados. São, ainda, considerados extremamente importantes, afinal, o contexto das redes sociais é formado por esse tipo de estrutura de dados. Basta que estes dados estejam armazenados e sob o controle de softwares chamados sistemas gerenciadores de bancos de dados.

Podem ser considerados bancos de dados: arquivos de texto, planilhas eletrônicas e estruturas de sistemas gerenciadores de bancos de dados. Estas últimas são armazenadas em forma de tabelas relacionadas entre si e representam objetos de um determinado negócio de uma empresa.

Os bancos de dados são importantes porque os sistemas de informação processam os dados ali armazenados. Ou seja, eles registram, alteram, disponibilizam para visualização e os deletam. Estes dados, portanto, se transformam em informação com um valor para uma empresa, isto é, ativos digitais. Eles passam, assim, a ter valor financeiro para a manutenção e a existência dos negócios de qualquer tipo de organização, seja privada ou pública.

1.6 Log

Quando o capitão de um navio escreve o diário de bordo (em inglês *log*), ele registra os principais fatos ocorridos na embarcação. Ele está na realidade fazendo este registro para a qualquer momento da navegação revisar o que aconteceu durante o período.

Da mesma maneira, os sistemas de uma rede, entre eles os gerenciadores de banco de dados, realizam constantemente o log de toda e qualquer operação ocorrida continuamente. Dessa maneira, eles garantem que todas as informações sejam registradas, informando quem acessou, quando, como, o valor da informação e que operação foi realizada.

O registro de *log* permite, em caso de perda de dados, que os sistemas de informação possam recuperar estes dados a partir do momento anterior à ocorrência da perda, para auditar as operações realizadas. Ou seja, validar quem acessou, o que foi feito sobre os dados e quando.

A existência de *log* é de extrema importância, como veremos no decorrer do livro, para os processos de segurança da informação.

Amplie seus conhecimentos

Os sistemas gerenciadores de bancos de dados possuem características em suas estruturas de dados, possuem também linguagens e regras para que as informações sejam extraídas dos mesmos, e os sistemas de informações utilizam dados para entrada que, processados, registram nos bancos de dados e os apresentam e disponibilizam para consultas por meio da linguagem SQL. Todas as operações realizadas com utilização de sistemas gerenciadores de bancos de dados são registradas em logs.

Pesquise em livros sobre Fundamentos de Bancos de Dados, ou na internet alternativamente, sobre o funcionamento e como são criados e mantidos os dados em sistemas gerenciadores de banco de dados e procure conhecer quais são os fatores relevantes em segurança da informação no tocante a banco de dados.

De nada servirá um sistema de segurança, por mais completo que seja, se os usuários, por exemplo, permitirem o acesso não autorizado ou fornecerem seu nome de usuário e senha a pessoas de fora da empresa, ou até a colegas da própria empresa, que não estejam habilitadas para tal fim, deixando aberta uma porta para ataques ou vazamentos de informações.

No mundo real, os aspectos sociais podem interferir diretamente no funcionamento de um sistema de informação.

Os procedimentos de operação e os acessos de um sistema de informação podem ser alterados ou refeitos em consequência direta de alguns aspectos sociais e de negócio, com objetivo de disponibilizar a existência de um maior controle dos acessos e das operações permitidas a usuários e realizadas sobre os dados que são objeto do sistema. Regulando assim a forma como são utilizados e manipulados.

Tudo o que é feito sobre dados depende do ambiente social em que estes dados estão disponibilizados e controlados.

1.7 Sociedade e segurança da informação

Atualmente estamos, e necessitamos estar, conectados. Ao ler um artigo na *Info Exame* sobre a internet, “?Não, Caiu!”, observamos o quanto estamos dependentes do “*estar conectado*”.

Temos a necessidade de ler e-mails, acessar dados de trabalho na empresa, efetuar pesquisas, ou mesmo ver um mapa para localizar um endereço ou um local aonde queremos chegar.

“Vivemos na internet e da internet”, diz Dagomir Marquezi, colunista da *Info Exame*.

É muito importante saber que, quanto mais interconectado nós, ou uma empresa, estivermos maior será a complexidade por onde trafegam e onde estão armazenadas as informações. E, consequentemente, maior deverá ser a preocupação com o nível de segurança a ser implantado para garantir os três princípios básicos da segurança: confidencialidade, integridade e disponibilidade.

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT, 2005, p. 2)

Não seria exagerado afirmar que as informações na sociedade dependem cada vez mais dos sistemas de informação e da utilização de computadores pessoais e equipamentos móveis. E, por isso, interpretamos a segurança da informação como assunto diretamente relacionado com a tecnologia da informação.



Figura 1.3 – Hacker.

Diariamente, lemos e ouvimos notícias sobre ataques realizados por piratas digitais.

São os hackers e crackers, que aparecem em centenas pelo mundo e realizam ataques a sites de empresas e organizações governamentais. Eles invadem sites de bancos, grandes redes de comércio virtual, entidades internacionalmente conhecidas como FBI, NSA, sites de governos estrangeiros, entre outros.

Hacker é uma pessoa que estuda, em profundidade, como modificar os aspectos internos de dispositivos de tecnologia da informação, programas e redes de computadores.

Com o aprimoramento desses conhecimentos, um hacker, com certa facilidade, consegue obter domínio e penetrar em equipamentos de rede, sistemas de informação, causando efeitos extremamente danosos a empresas e pessoas. Ele, inclusive, consegue superar as barreiras que são criadas para impedir o acesso e controle externo de sistemas de informação e de bancos de dados que são utilizados por este sistema.

Às vezes, o conceito de **hacker** se confunde com um outro tipo de estudioso com as mesmas capacidades, mas com objetivos diferentes. Trata-se dos crakers.

Segundo a definição correta, hacker é aquele indivíduo que se preocupa em utilizar seu conhecimento para detectar e melhorar falhas e vulnerabilidades de sistemas de informação e redes de computadores.

Por outro lado, os crackers, com seu conhecimento e nenhuma preocupação em manter o funcionamento de sistemas de informações, são os atacantes de sistemas preocupados principalmente em deixar uma “marca”, bloquear acessos, roubar informações ou simplesmente destruir completamente um sistema.

Cracker (quebrador) deveria ser utilizado somente para identificar aqueles indivíduos que praticam a quebra (ou cracking) de um sistema de informações e de sua segurança, de forma ilegal e antiética.

Entretanto, vulgarmente o termo hacker ficou associado às pessoas que têm o domínio especializado e profundo de sistemas operacionais, redes e linguagens de programação, em nível de

como se dão os processamentos internos em computadores. São eles que invadem sites, criam vírus e quebram a segurança de sistemas.

Nesse caso, o mais correto seria utilizarmos craker como o substantivo que define os mal-intencionados e hacker como os bem-intencionados.

Quando alguém deseja baixar um software e utilizá-lo como cópia pirata, esta pessoa procura normalmente um crack (quebra) para este software, ou seja, um código que quebra a segurança da licença de uso deste software. Assim, ela poderá utilizá-lo sem ter adquirido e pago os direitos de licenciamento pelo seu uso.

Fica claro, então, que craker é quem pratica o roubo de dados e altera sistemas de informação. Enquanto isso, quem busca identificar vulnerabilidades e criar proteções para elas são os hackers.

Infelizmente popularizou-se o termo hacker. Contudo, para não nos distanciarmos tanto do senso comum, chamaremos, neste livro, de hackers todos que atacam redes e sistemas de informação.

Amplie seus conhecimentos

Mark Zuckerberg, criador do Facebook, começou sua carreira como um hacker. Ele invadia o banco de dados dos alunos da Universidade de Harvard com o objetivo de fornecer uma forma mais simples de as pessoas se conectarem entre si, alterando o chamado Anuário Online que continha dados sobre os estudantes da Universidade. O site alterado combinou os elementos de um anuário comum já existente com mais funções para os perfis, permitindo que os estudantes buscassem uns aos outros de acordo com cursos, organizações sociais e dormitórios. Assim nasceu o TheFacebook.

Procure, portanto, pesquisar mais sobre como o Facebook foi criado, sobre a trajetória de Zuckerberg, um hacker que mudou e criou uma das maiores corporações de negócios da internet nos dias de hoje.

No Google, há diversos sites com curiosidades e histórias da carreira de Zuckerberg e como ele se tornou uma referência para o assunto.

Antigamente acreditava-se que os hackers eram pessoas que queriam se vingar de alguma empresa, ou adolescentes que queriam ser aceitos por grupos de hackers (ou script kiddies)² e saíam apagando tudo que encontravam. Ou, ainda, eram grandes

especialistas de linguagens de programação que eram contratados por algumas empresas para fazerem espionagem industrial, invadindo redes e sistemas de empresas concorrentes.

Hoje em dia ainda existe, por exemplo, a superstição de que empresas que produzem antivírus possuem em suas equipes hackers para criar vírus e disseminá-los em âmbito mundial. Com isso, elas criariam e distribuiriam as chamadas “vacinas” contra estes mesmos vírus.

1.7.1 Notícias de segurança da informação

Diariamente sabemos de uma novidade bombástica no universo virtual da internet.

Em 2013, um dos assuntos que mais chamou atenção quanto ao acesso a informações de pessoas e empresas foi o caso Snowden:

Ex-agente da Agência de Segurança Nacional dos Estados Unidos (NSA), Edward Snowden revelou que ele mesmo espionava e acompanhava, para a NSA, tudo o que eu, você ou praticamente qualquer outra pessoa fazem na internet.

Chamado de Prism, este sistema secreto (?) receberia a colaboração de empresas de telefonia e também de algumas das maiores companhias digitais do mundo, como Facebook, Microsoft®, Apple® e Google®.

Snowden denunciou as práticas de espionagem em uma entrevista porque, segundo ele, “quem deve decidir se os governos devem – ou não – investigar o que as pessoas comuns fazem na internet são os próprios cidadãos”.

A divulgação deste fato alertou pessoas e organizações de vários países para uma prática de ações de espionagem, as quais já se desconfiava estarem sendo realizadas há muito tempo.

Depois de as denúncias terem sido feitas e documentos terem sido apresentados, comprovando as ações de monitoramento realizadas, “caiu a ficha” de todo mundo. Sim, estamos sendo monitorados em quase tudo o que fazemos na internet.

Explicaremos tudo o que envolve o Prism e sua privacidade, leitor, ao navegar na internet. Isto nos ajudará a entender o porquê da necessidade e importância tão grande de segurança da informação, assim como por que regras, políticas e ferramentas de segurança podem ser eficientes de fato.

Em artigo publicado no site TecMundo, Lucas Karasinski explicou detalhadamente como funciona, ou funcionava, o Prism, este sistema de monitoramento de atividades na internet no mundo inteiro.

Segundo Lucas, o jornal americano *Washington Post* e o inglês *The Guardian* apresentaram dois artigos que impressionaram e revelaram muito sobre o grau de segurança das nossas informações e de governos e empresas ao redor do mundo.

Este assunto obviamente foi o sistema Prism, um projeto de colaboração secreta entre NSA, FBI e quase todas as empresas de tecnologia em que confiamos e usamos diariamente.

O Prism forneceu ao governo dos Estados Unidos acesso sem precedentes a informações pessoais, pelo mundo, há pelo menos seis anos. Mas qual é o significado disso, exatamente? Para Lucas Karasinski:

O Prism é na verdade uma sigla para um programa real do governo dos Estados Unidos. De acordo com documentos vazados, ele entrou em ação em 2007, e só ganhou força desde então.

A sua finalidade é monitorar potenciais comunicações estrangeiras valiosas que podem passar pelos servidores dos Estados Unidos, mas parece que na prática seu alcance é bem maior.

Os relatos iniciais sugeriam que o processo funcionava da seguinte maneira: as empresas anteriormente mencionadas (e talvez até outras) recebiam uma diretiva do procurador-geral e do diretor de inteligência nacional.

Elas davam acesso aos seus servidores através da Unidade de Tecnologia de Interceptação de Dados do FBI, a qual por sua vez os retransmitia para os escritórios de tecnologia da NSA.

Ainda existem, como você deve imaginar, filtros para ajudar a lidar com a quantidade de dados recebidos diariamente, os trilhões de bits e bites que fazem sua identidade e vida online.

Alguma coisa para garantir que apenas os caras maus estão sendo vigiados (será?), e não os cidadãos honestos. Existe sim um filtro, e é ridículo: um analista da NSA precisa ter 51% de certeza de que um assunto é “externo”. Depois disso, carta branca.



Provedores atuais



O que é recebido na captura



Figura 1.4 – Dados Coletados pelo Prism.

O que é mais preocupante sobre o PRISM não é a coleta de dados.

É o tipo de dado coletado.

De acordo com o artigo do *Washington Post*, isso inclui:

...conversas por vídeo e áudio, fotografias, e-mails, documentos e logs de conexão... [Skype®] podem ser monitorados por áudio quando um dos lados da conversa é em um telefone convencional, e para qualquer combinação de ‘áudio, vídeo, chat, e transferência de arquivos’ quando os usuários do Skype® se conectam por um computador.

O disponibilizado pelo Google inclui Gmail, chats de voz e vídeo, arquivos do Google Drive, bibliotecas de fotos e vigilância de termos de busca em tempo real.

Veja o quanto de suas informações estão acessíveis nesta situação.

A mesma profundidade similar de acesso também se aplica ao Facebook, Microsoft e ao resto.

Para sermos mais claros: isso abrange praticamente qualquer coisa que você já tenha feito online, e ainda inclui pesquisas no Google® enquanto você está digitando.

Quando a NSA monitora registros de telefone, ela só coleta os metadados deles. Isso significa quem e para quem a chamada foi feita, e de onde ela foi feita, e outras informações gerais.

É importante entender que, até onde sabemos, o conteúdo das conversas não era monitorado ou registrado.

Em contraste, o PRISM pelo noticiário geral que se tem acesso permite acesso total não apenas ao fato de que um e-mail foi enviado – ele permite acesso ao conteúdo destes e-mails e chats.

E observe que, como veremos em capítulo específico de controles de segurança, os e-mails enviados por qualquer pessoa são normalmente criptografados, o que impediria outros de os lerem sem chave para decodificá-los. Entretanto, isso acontece porque todas as pessoas utilizam as chamadas chaves públicas que são mais simples de serem decodificadas.

De acordo com a fonte do *Washington Post*, eles podem “*literalmente vigiá-lo enquanto você digita*”. Eles podem estar fazendo isso com você, agora mesmo.

1.7.2 As tendências em segurança

Com o crescimento do uso de sistemas de informação, comércio eletrônico e tecnologia digital, as empresas e as pessoas estão se vendo obrigadas a pensar mais na segurança de suas informações para superar ameaças e golpes, a que estamos expostos todos os dias.

Assim, podemos entender que a segurança da informação veio para minimizar possíveis ataques aos sistemas empresariais e domésticos.

Simplificando, a segurança da informação é uma maneira de proteger os sistemas de informação e a sociedade contra diversos ataques, mantendo documentos e arquivos dentro dos princípios de confidencialidade, integridade e disponibilidade.

Os problemas de segurança da informação são em geral provocados por pessoas mal-intencionadas que buscam algum tipo de vantagem, seja ela monetária, política, intelectual etc.

Existe alguma maneira rápida e eficiente de se descobrir uma senha?

Simplesmente perguntar? Ou observar alguém digitando a senha e decorar?

Por mais incrível que isso possa ser, é esta a forma mais simples, mais usada e provavelmente a mais eficiente de se obter informações: simplesmente chegar e perguntar.

Nos próximos capítulos falaremos sobre os ataques e golpes que deram origem a uma área específica da segurança da informação tanto em empresas quanto em nossos computadores, smartphones e tablets.

1.7.3 Mais notícias para você

EA sofre ataque DDoS³, e servidores da Origin ficam fora do ar (6 de jan. de 2014).

Este ataque de negação de serviço certamente foi realizado ao servidor da EA (Electronic Arts), o que derruba os servidores da Origin, e pelo tipo de ataque deve ter impedido os jogadores online no mundo de acessar os serviços desta plataforma de distribuição de games.

Com este ataque, os jogadores no mundo inteiro ficaram durante um tempo impossibilitados de fazer login no serviço de games online e, óbvio, não podiam jogar os games desta empresa em diversos equipamentos de vídeogame, incluindo o PC, Xbox 360 e Xbox One, ou até realizar compras na loja online deste site.

Claro que, com um ataque deste, após a realização de manutenção, tudo voltou a funcionar normalmente.

Fonte: Olhar Digital. Acesso em: 3 jan. 2014.

No final de 2013, uma das maiores redes de varejo dos Estados Unidos, em plena época de compras de Natal, viu os dados de cartões de crédito de milhares de clientes serem vazados após os sistemas da empresa terem sido invadidos por hackers. O ataque foi amplamente divulgado em todas as mídias.

Fique de olho!

Ameaças virtuais criadas para tirar vantagem da confiança de usuários em sistemas, aplicativos e redes pessoais alcançaram níveis alarmantes, apontou relatório de segurança da CISCO®. Ainda segundo este fabricante de equipamentos de rede e segurança, as vulnerabilidades e ameaças chegaram ao nível mais alto desde que começou o rastreamento no ano de 2000.

A quantidade de alertas de segurança aumentou 14% no ano passado.

Trojans (falaremos sobre eles a seguir) foram os malwares encontrados com mais frequência, com 27% do total detectado no ano passado. Nos dispositivos móveis, programas mal-intencionados estavam em lojas não oficiais dos sistemas operacionais destes dispositivos.

Há dois anos aproximadamente os principais jornais e meios de comunicação mundiais divulgaram notícias sobre um desconhecido site chamado de WikiLeaks.

O conteúdo apresentado pelo site (documentos secretos de vários países) causou grande repercussão no mundo inteiro. Chegou-se, inclusive, a falar no início da primeira ciberguerra da história. Entretanto, este mesmo conteúdo, de caráter político, colocou em situação constrangedora alguns países no que diz respeito aos direitos humanos, trazendo a público questionamentos sobre como muitos países se posicionam frente a este fato.

O WikiLeaks foi fundado em 4 de outubro de 2006, na Suécia, e construído sob a plataforma de MediaWiki, similar ao da Wikipédia.

O conteúdo do site tem a opção de edição restrita a um seletº grupo de editores, cujo principal editor era o jornalista e ciberativista australiano Julian Assange. Era ele quem publicava a maior parte dos documentos, tornando-se famoso em 2010 com a divulgação de arquivos secretos do governo dos Estados Unidos da América, como documentos relativos à Guerra do Afeganistão e à Guerra do Iraque. Como característica comum, muitos desses documentos denunciavam graves violações aos direitos humanos.

Para especialistas, até mesmo o conteúdo de um site como o WikiLeaks pode ser objeto de uma inclusão de dados fraudulenta. Isso acontecerá se alguma informação for ali postada e esta mesma

informação for adulterada visando apenas causar impacto na população e na comunidade internacional, sem ter fundamento verídico.

Continuaremos estudando o que afeta a segurança da informação e buscaremos conhecer melhor as ameaças e problemas que tanto causam.

Existem diferentes áreas de segurança que afetam umas às outras e que são objeto do contexto geral denominado segurança da informação.

A segurança física está inter-relacionada com a segurança da informação, a segurança dos bancos de dados, e no topo desta cadeia encontra-se a segurança do sistema operacional.

À segurança implica diretamente na forma como as operações com sistemas são utilizadas nas empresas.

Tecnologia, hardware, pessoas e procedimentos importam em conjunto como fatores para a segurança da informação, assim como aspectos ambientais, entre eles: terremotos, enchentes, raios, quedas de energia, incêndios etc.

Nos próximos capítulos estudaremos as vulnerabilidades para a segurança da informação.

Vamos recapitular?

Neste capítulo, apresentamos os conceitos básicos da segurança da informação, inclusive mostramos a diferença entre informação e dado. Além disso, demos exemplos de casos graves de violação de segurança.

Mostramos também que existem duas denominações para designar as pessoas que executam estas violações, apesar de uma ser a mais utilizada.

Falamos também que não são somente pessoas que causam problemas para a segurança da informação. Devemos levar em conta aspectos físicos, climáticos e os chamados lógicos, provocados por especialistas ou não.



Agora é com você!

- 1) Pesquise em livros, jornais, revistas e na internet um caso recente de indisponibilidade de informações, perda de confidencialidade ou invasão de sites, e faça uma descrição resumida de três parágrafos sobre o fato ocorrido e quais danos foram causados por violação destes princípios de segurança da informação.
- 2) Assista a um seriado de televisão em que alguém acessa dados, por exemplo do FBI, e responda qual dos princípios está sendo violado no seu entendimento.
- 3) Violação de acesso (acesso não autorizado) com utilização de senha de um amigo ou colega viola qual princípio, conforme apresentado no início deste capítulo?
- 4) Qual a denominação para quem acessa dados não autorizados, destrói dados ou rouba informação de redes, sistemas e computadores?
- 5) O sistema Prism da agência americana NSA, tão comentado nas notícias, violou ao interceptar mundialmente mensagens e conversas na internet qual dos princípios da segurança da informação?
- 6) Demonstre com três exemplos que não estejam no livro a diferença entre informação e dado, no formato da tabela a seguir:

Informação	Dado
------------	------

-
- ¹ Surf de ombro é quando uma pessoa olha por cima do ombro de outra pessoa e observa a sua digitação ou os dados que aparecem na tela.
 - ² Script Kiddies significa garoto dos scripts, em tradução literal. É um termo depreciativo atribuído aos grupos de crackers inexperientes que desenvolvem atividades relacionadas com segurança da informação, utilizando-se do trabalho intelectual dos verdadeiros especialistas técnicos. Eles não possuem conhecimento de programação e não estão interessados em tecnologia, e sim em ganhar fama ou outros tipos de vantagens pessoais.
 - ³ Um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service) é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Falaremos um pouco mais sobre o assunto mais à frente.

2

Redes e Internet

Para começar

Este capítulo tem por objetivo apresentar os conceitos básicos sobre o ambiente de redes, isto é, o principal ambiente onde devemos nos preocupar com a segurança da informação.

Estudaremos quais são os principais tipos de redes utilizadas, como funciona o acesso à internet a partir de uma rede ou até mesmo de seu computador doméstico, como os computadores localizam uns aos outros e como um nome de site é identificado na rede mundial. Abordaremos, ainda, os conceitos e como funcionam as redes e a internet.

2.1 Acesso a uma rede

Para um usuário ser capaz de acessar um recurso de uma rede, deve-se confirmar se esse indivíduo é quem ele afirma ser, se ele tem as credenciais necessárias e se ele tem os direitos ou privilégios necessários para executar as ações desejadas.

Uma vez que não haja qualquer problema com estes requisitos, o usuário pode acessar e realizar ações utilizando os recursos de uma rede de computadores. Entretanto, é necessário que as atividades deste usuário sejam rastreadas, assim como sejam registradas a responsabilidade pelas ações que o mesmo vier a realizar.

Identificação é um método para garantir que um objeto (usuário, programas ou processo) é o que informa ser. Ou seja, um usuário, um programa de sistema ou um processo interno do computador ou da rede deve possuir uma identificação para que as atividades executadas por ele possam ser registradas.

Mas, antes de seguirmos com estes conceitos, vamos revisar um conceito importante para o entendimento geral do assunto:

O que é uma rede de computadores? Onde vamos aplicar os conceitos como Identificação, Autenticação, Autorização e Contabilização?

2.2 O que são redes de computadores

Nosso objetivo aqui é apresentar noções gerais sobre o que é uma rede de computadores. Não pretendemos nos aprofundar nos conceitos, topologias e conhecimento técnico de redes, apenas o suficiente para entendermos a aplicação da segurança da informação em um ambiente que tanto pode ser o doméstico, com uma rede wireless (sem fio) para conexão a internet por banda larga, ou a rede de uma empresa.

Uma rede de computadores nada mais é que um grupo de computadores com funcionamento independente um do outro e interconectados por cabos de rede, ou com um computador denominado servidor de rede.

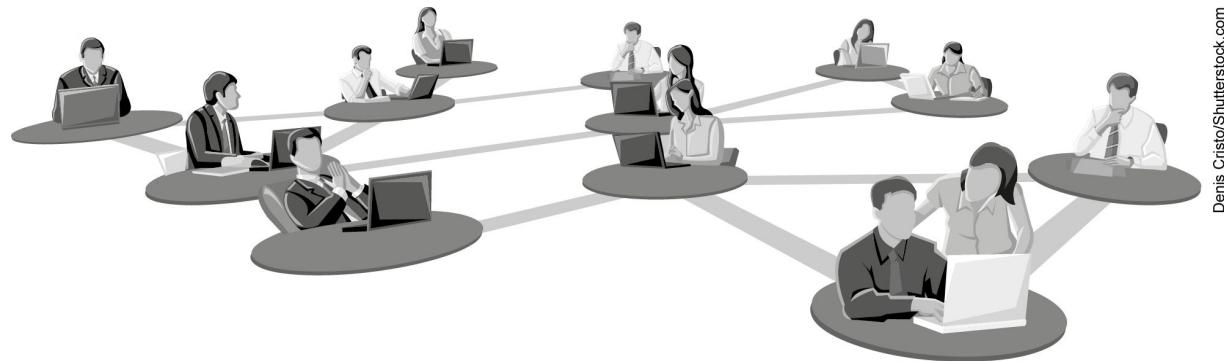


Figura 2.1 – Uma rede.

A rede permite o compartilhamento de softwares, [informações](#), [arquivos](#) e demais serviços. Nela, por exemplo, pode-se ter acesso a arquivos, softwares ou impressoras que estejam em outro computador. Ele pode atuar, portanto, em computadores e periféricos (impressoras, scanners, entre outros equipamentos).

Uma rede de computadores é um sistema de comunicação de dados constituído por meio da interligação de computadores e outros dispositivos, com a finalidade de trocar informações e compartilhar recursos.

Uma rede básica de computadores consiste em dois computadores interligados com o objetivo de compartilhar dados. Em se tratando de uma rede de trabalho, por outro lado, é um sistema que permite a comunicação entre pontos distintos e a troca que permite a troca de informações.

Os componentes básicos de uma rede de trabalho (ou rede de informações) são um equipamento emissor (origem da informação), o meio através da qual a informação trafega (o canal), um equipamento receptor (o destino da informação) e finalmente a mensagem, que é a informação em si.

Um exemplo do mundo real é uma pessoa falando ao telefone com outra pessoa. O emissor seria quem está falando e o aparelho de telefone; o canal de comunicação seria a linha telefônica; o receptor, a pessoa e o aparelho de telefone de quem está ouvindo; e como mensagem entendemos ser aquilo que está sendo conversado, as palavras enviadas de um para o outro.

Redes de computadores são compostas por uma série de equipamentos eletrônicos necessários à interconexão de dispositivos, como microcomputadores e impressoras. Esses dispositivos que se comunicam entre si são denominados nós de rede, estações de trabalho, pontos ou simplesmente dispositivos de rede.

Dois computadores, ou nós, seriam o número mínimo de dispositivos necessários para formarmos uma rede. O número máximo não é predeterminado. Teoricamente todos os computadores do mundo poderiam estar interligados.

Normalmente temos dois tipos de redes de computadores:

- » cliente-servidor (client-server)
- » ponto a ponto (peer-to-peer)

Na rede cliente-servidor, uma máquina, ou um pequeno grupo de máquinas, centraliza os serviços da rede oferecidos às demais estações, como aplicativos e serviços de impressão.

As máquinas que requerem esses serviços são chamadas de clientes, e as máquinas que os fornecem, servidores.

Na rede ponto a ponto não existem servidores. Todas as estações compartilham seus recursos mutuamente.

Para entendermos melhor a diferença entre os tipos de rede: nas redes ponto a ponto é quase impossível gerenciar os seus serviços, já que não existe um sistema operacional que centralize a administração da rede e seus clientes como em uma rede cliente-servidor.

Como o nome sugere, a rede ponto a ponto é a ligação entre um computador e outro diretamente, ou utilizando um canal como intermediário, porém sem controles de gerenciamento completo, sobre como está sendo realizada a utilização dos recursos e das informações trocadas entre eles. Um exemplo disso são as redes tipo mTorrent e BitTorrent, utilizadas para baixar filmes, músicas e arquivos em programas como o Ares (software livre), que funcionam como se existisse um cabo ligando dois computadores.

O uso das redes, em especial da internet, tem disponibilizado uma variedade de oportunidades para as empresas, e novos mercados para sua atuação são alcançados.

2.2.1 Objetivos de uma rede

Podemos destacar como os principais objetivos de uma rede:

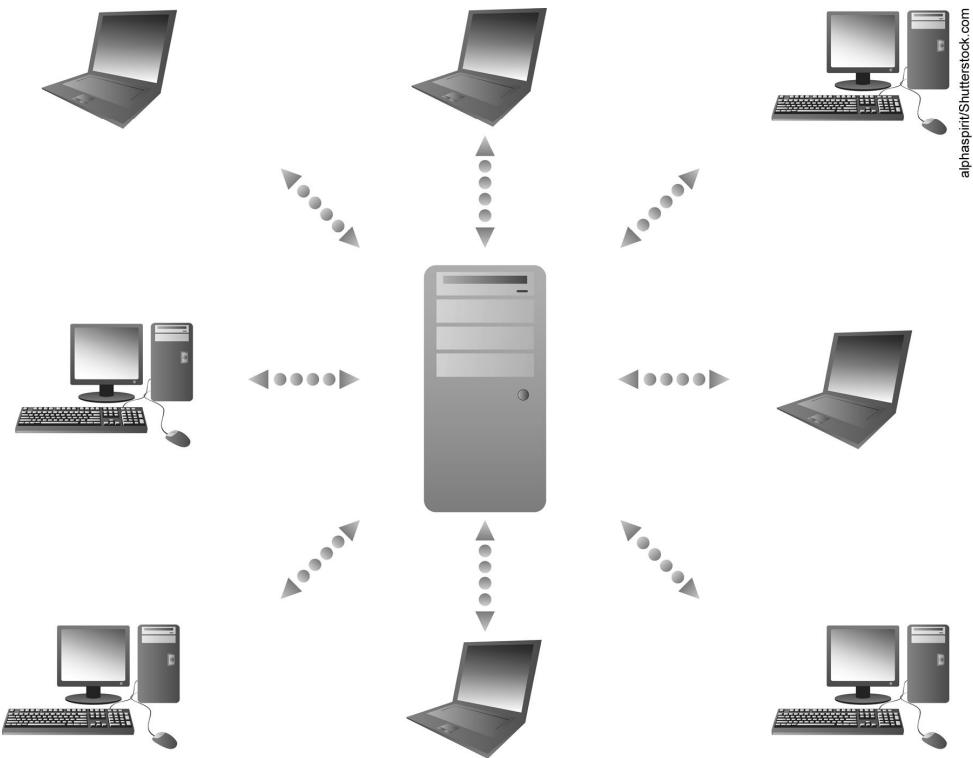


Figura 2.2 – Objetivos de uma rede.

- 1) Tornar todos os programas, dados e outros recursos disponíveis a todos os usuários, sem considerar a localização física do recurso, seja na empresa matriz, em sua filial, ou em qualquer outro lugar;
- 2) Fornecer um meio de comunicação eficiente para troca de informações entre pessoas ou empresas.

Um termo muito comum no mercado atual é o chamado ambiente colaborativo, no qual clientes e fornecedores interagem por meio de redes, utilizando para esta comunicação a rede mundial da internet. Nesses casos, é permitido que um cliente tenha acesso a determinados processos e programas da empresa fornecedora,

assim como uma empresa cliente pode ter acesso direto à rede do fornecedor para realizar um pedido de compras no sistema de vendas desta.

Hoje, a comunicação entre pessoas e departamentos dos usuários de uma empresa, utilizando-se de mensagens de e-mail, tornou-se uma necessidade para simplificar a operação de negócio do dia a dia.

Antigamente, quando uma impressora que estava ligada a um computador de um usuário do setor de cobrança, por exemplo, ela não podia ser utilizada por um usuário de setor de vendas, que não ficava localizado junto ao setor de compras. Era necessário, então, que este usuário do setor de vendas se deslocasse até o setor de cobrança com o arquivo, em um disquete na época, para realizar a impressão.

Hoje, até mesmo em nossa casa, com rede Wi-Fi doméstica, podemos ter somente uma impressora e todos os computadores que estiverem compartilhando esta rede utilizarão a mesma impressora.

É sobre estes ambientes em que a segurança da informação atua para garantir os princípios que abordaremos mais detalhadamente no capítulo seguinte. Além disso, falaremos sobre como se proteger das ameaças que rondam e tentam perturbar os serviços nos ambientes de redes.

O tema redes é muito abrangente e encantador de ser estudado. Porém apresentaremos somente alguns conceitos necessários ao entendimento das ameaças à segurança da informação e as suas formas de prevenção, detecção e eliminação, seja de redes domésticas ou de empresas.

2.2.2 Protocolos de comunicação de redes

Os protocolos de rede são um dos recursos técnicos utilizados para estabelecer a comunicação entre os computadores que estão interconectados por meio de uma rede.

Para entendermos melhor o que são os protocolos de rede, vejamos um exemplo prático: pensemos em um coreano que não fala português e um brasileiro que não fala coreano. Ambos podem se comunicar usando uma língua em comum, como o inglês, que seria algo como um protocolo de comunicação entre os dois. Entretanto, mesmo que ambos não falassem nenhuma língua em comum, eles poderiam usar gestos universais para tentar se comunicar.

Os protocolos são justamente como essas línguas e sinais universais que permitem aos dispositivos comunicar-se por intermédio da rede.

Assim como há várias línguas no mundo, nos ambientes de rede existem diversos protocolos. Neste livro, analisaremos o protocolo TCP (na sigla em inglês, *Transmission Control Protocol*), ou Protocolo de Controle de Transmissão, e o Protocolo de Interconexão ([Internet](#) Protocol), que são abreviações dos principais protocolos que compõem o chamado TCP/IP. Estes dois protocolos formam a linguagem de comunicação principal entre computadores de uma rede.

2.2.3 Endereço IP

Como os computadores, ou smartphones, conseguem acessar páginas na Web ou receber um arquivo de download? Ou, ainda, como, na rede de uma empresa, um computador se comunica com a máquina de alguém em outro andar?

Essas ações acontecem porque, tanto em redes locais quanto na rede mundial de computadores (*i.e.*, a internet), cada dispositivo conectado tem um endereço único: o **IP**, sigla para **Internet Protocol**.

Portanto, o que é endereço IP?

Um endereço IP é o número que identifica exclusivamente um dispositivo conectado a uma rede TCP/IP.

Esse endereço é formado por uma sequência de números compostos de 32 bits, divididos em quatro grupos de 8 bits que recebem o nome de *octeto*, porque cada um deles tem oito posições quando visualizados na forma binária.

Com 8 bits, são permitidas de serem realizadas até 256 combinações diferentes em cada um destes grupos. E para que esta configuração seja delimitada e facilitada, são utilizados os números de zero a 255 para representar cada octeto, porque é mais fácil formar números como 74.86.238.241 do que utilizar números binários em um octeto de 8 bits, como 01001010.01010110.11101110.11110001.

Com o endereço IP, podemos inclusive identificar a região ou país no qual um computador está conectado à internet.

Não devemos confundir endereço IP com endereço MAC (endereço físico), que é um número hexadecimal fixo atribuído pelo fabricante da placa de interface de rede, uma placa que existe no computador. Em um computador de mesa (estação de trabalho), é onde estará conectado um cabo azul de rede, como a Figura 2.3.

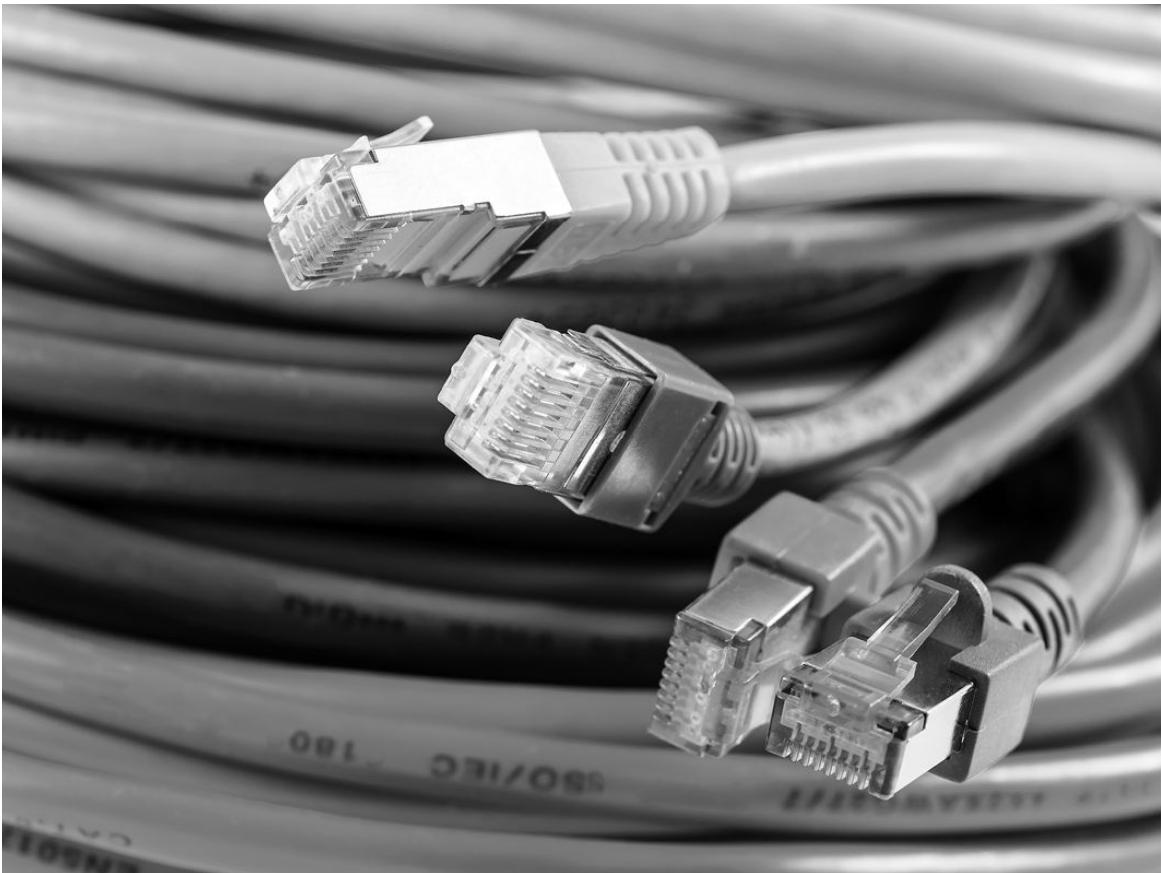


Figura 2.3 – Cabos de rede.

O endereço IP pode ser fixo (IP estático) ou mudar a cada conexão (IP dinâmico). Mas sempre deve permitir que um computador possa localizar outro computador na rede.

Agora estudaremos o que é um host!

2.2.3.1 Hosts

Host é qualquer computador ou máquina conectado a uma rede. É ele o responsável por oferecer recursos, informações e serviços aos usuários ou computadores clientes.

Por ser um termo abrangente, pode ser utilizado como designação para diversos casos que envolvam um computador e uma rede.

Endereços IP também são atribuídos a um host no momento da inicialização, ou permanentemente pela configuração fixa de seu hardware ou software.

Configuração *persistente* é também conhecida como a utilização de um endereço de IP estático, ou seja, um endereço que é sempre o mesmo independentemente da inicialização do computador.

Por outro lado, nas situações em que o endereço de IP do computador é atribuído a cada inicialização, e é realizada uma conexão a uma rede, isto é conhecido como sendo a utilização de um endereço de IP dinâmico.

Digamos que você queira enviar uma carta a alguém, você... Ok, você não envia mais cartas. Prefere enviar e-mails ou deixar um recado no Facebook.

Vamos então melhorar este exemplo. Quando desejamos enviar um presente a alguém, obtemos o endereço da pessoa e contratamos os Correios ou uma transportadora para entregá-lo.

É graças ao endereço do destinatário que encontramos geograficamente a pessoa a ser presenteada. Também é graças ao endereço de remetente que se identifica quem enviou o presente, um endereço que também é único para cada residência ou estabelecimento.

Da mesma forma que recebemos nossa conta de água, também recebemos um produto comprado em uma loja online, porque houve um endereçamento referente à nossa residência.

Em uma rede ou na internet, o princípio é o mesmo. Para que um computador seja encontrado e possa fazer parte de uma rede corporativa ou da rede mundial de computadores, ele necessita ter um endereço único.

O mesmo vale para websites, como o Google, que fica em um servidor, ou melhor, em uma quantidade imensa de servidores interligados que precisam ter um endereço para serem localizados na internet. Vale relembrar que isto é feito pelo endereço IP (*IP Address*), mesmo recurso utilizado para redes locais, como a existente em uma empresa.

Como já vimos, o endereço IP é uma sequência de números composta de 32 bits.

Esse valor consiste em um conjunto de quatro sequências de 8 bits.

Cada uma destas sequências é separada por um ponto.

O número **172.31.110.10** é um exemplo.

Repare que cada octeto é formado por números que podem ir de zero a 255, que são delimitadores, não mais do que isso.

A divisão de um endereço IP em quatro partes facilita a organização da rede, da mesma forma que a divisão do seu endereço em cidade, bairro, CEP, número etc., e torna possível a organização das casas da região onde você mora.

O CEP, por exemplo, agrupa vários endereços de residências em uma área da cidade, lado da rua etc. Analisando veremos que os dois primeiros dígitos de um CEP indicam o estado do endereço. No Rio Grande do Sul todos os números de CEP começam com 90.

Neste sentido, os dois primeiros octetos de um endereço IP podem ser utilizados para identificar a rede e o host da rede.

172.31.110.10
1º octeto

Vamos considerar uma escola que tem uma rede para alunos e outra para professores. Pode-se ter 172.31.xxx.xx para uma rede e 172.32.xxx.xx para a outra, sendo que os dois últimos octetos são usados na identificação de computadores.

Mas observe que, nas duas redes, o número 172 identifica como rede da escola, sendo a de professores é a 32, ou seja 172.32.xxx.xx.

O conjunto da utilização destes endereços com o TCP compõe a linguagem, ou melhor, o protocolo, cuja denominação mais adequada é TCP/IP.

Agora já sabemos que os computadores, em uma rede, se comunicam tanto em uma rede interna de uma empresa quanto na internet por meio do “protocolo” TCP/IP.

A chamada World Wide Web (WWW) virou sinônimo de internet, mas na verdade a WWW é apenas um dos serviços disponíveis na internet. A World Wide Web é somente a parte gráfica da internet, que contém muitos outros serviços como SMTP (e-mail) e FTP (transferência de arquivos), sem falar em outros serviços, como o famoso compartilhamento de arquivos onde muita gente encontra arquivos de música MP3, vídeos, imagens, documentos etc.

Cada sistema de compartilhamento de arquivos tem seu próprio protocolo, que roda “por cima” do protocolo TCP/IP e que, por sua vez, forma uma espécie de esqueleto sobre o qual são construídos outros sistemas de transporte de dados, os chamados endereços IP.

Mas, além destes protocolos, como o computador consegue localizar estes sites, independente de onde estejam hospedados?

É neste ponto que “entra em cena” o trabalho dos servidores DNS (*Domain Name System*).

2.2.4 DNS – Domain Name System

Os endereços da internet são mais conhecidos pelos nomes associados aos endereços IP (por exemplo, o nome www.wikipedia.org está associado ao IP 208.80.152.1301). Para que isto seja possível, é necessário traduzir (resolver) os nomes em endereços IP e vice-versa. O DNS é um mecanismo que realiza esta conversão.

Já sabemos, então, que todo site tem um endereço IP. Agora, imagine que para navegar na internet fosse necessário decorar o número IP de todos os sites.

Para que não tenhamos essa dificuldade, possuímos o DNS, que associa um nome de domínio tipo www.google.com.br a um número IP, simplificando a forma de navegar na internet.

Os nomes DNS são hierárquicos e permitem que faixas de espaços de nomes sejam delegados a outros DNS. Chama-se isso de registro de domínio.

Neste ponto, você já sabe que os servidores de DNS têm papel importantíssimo na internet. O problema é que o DNS também pode ser “vítima” de ações maliciosas.

Imaginemos, por exemplo, que um hacker com grande conhecimento no assunto elaborou um programa para conseguir capturar solicitações de resolução de nomes de clientes de um determinado provedor, como um site de compras.

Se ele tiver sucesso, poderia direcionar um endereço falso no lugar de um site que um usuário queira visitar e realizar compras.

Perceba o risco: se o usuário não perceber que foi direcionado para uma página falsa, poderá fornecer dados sigilosos, como o número de cartão de crédito.

Para evitar problemas como estes é que foi criado o **DNSSEC** (*DNS Security Extensions*), que consiste em uma especificação que adiciona recursos de segurança ao DNS – estudaremos, mais à frente, este processo de segurança em mais detalhes.

Amplie seus conhecimentos

Como todo computador tem seu endereço IP, vamos mostrar a título de curiosidade como identificar o endereço IP de um computador.

Independentemente do Windows utilizado, clique em acessórios, prompt de comando. Em seguida, digite ipconfig. Será apresentada, então, uma nova tela com o número do seu IP:

192.168.25.194

Como você já estudamos como são as redes e como elas funcionam, mostraremos como computador, ou uma rede, se conecta à internet, e como chegar à página de um site qualquer.

Estes conceitos são importantes para a sequência de entendimento e aprendizagem da Segurança da Informação, pois estaremos cobrindo todos o conjunto de ambientes onde iremos estudar do que e como nos proteger.

2.2.5 Como funciona uma conexão à internet

Antes de mostrar para você como funciona uma conexão a um site na internet, vamos explicar como os computadores se conectam na rede por meio dos endereços IP e também como o servidor de DNS completa este ciclo de comunicação.

Existe um conceito chamado de topologia de rede.

A topologia é o nome que define como é feita uma estrutura de rede. Existem duas partes na definição da topologia, a topologia física e a topologia lógica.

A topologia física trata do layout, ou seja, a forma como os dispositivos ficarão dispostos/conectados na rede.

A topologia lógica define como os meios são acessados e a forma como os sinais trafegam pelos equipamentos. São três as mais importantes topologias de rede: a rede tipo barramento, a rede em estrela e a topologia em anel.

A topologia de barramento é quando todos os computadores estão conectados por um cabo comum a todos.

A topologia em barramento é simples, pois pode crescer conforme conectamos equipamentos ao cabo comum de rede. São as conhecidas redes chamadas Ethernet.

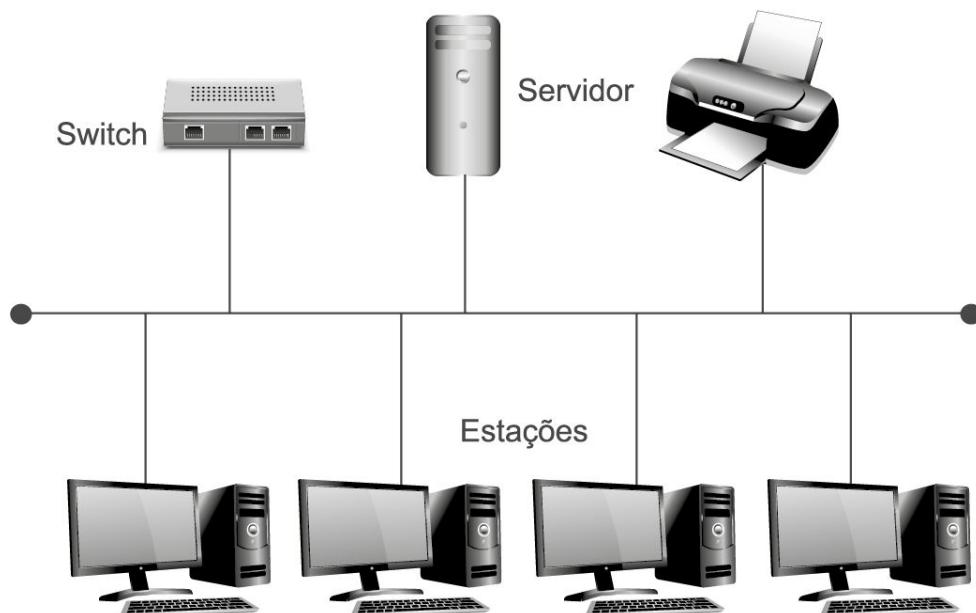
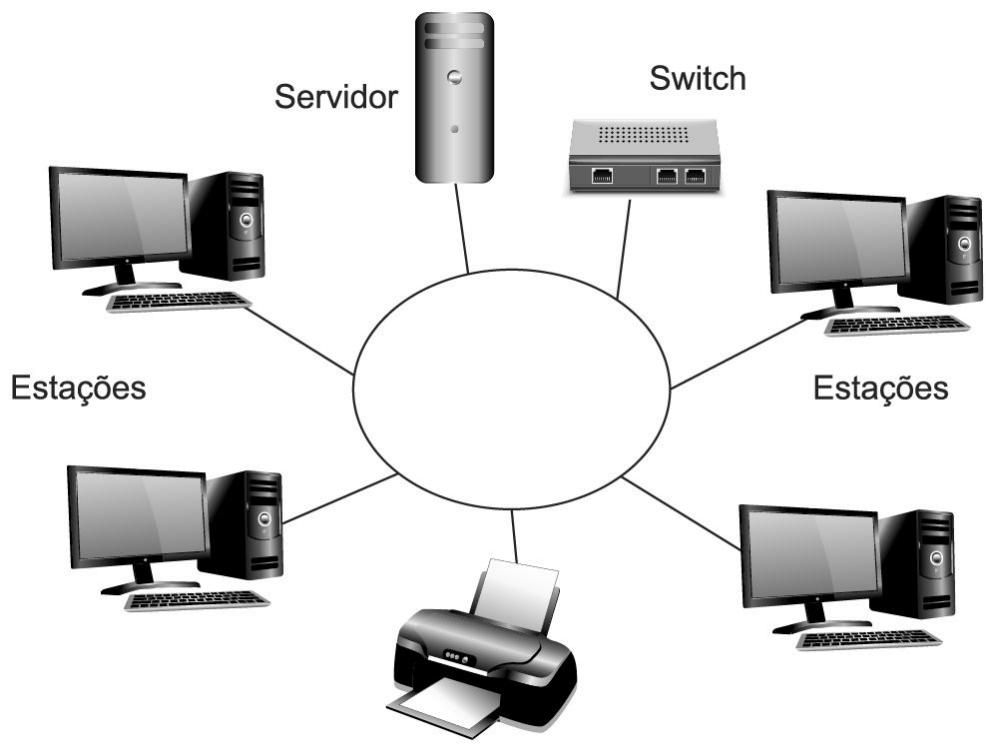


Figura 2.4 – Topologia de Barramento.

Entretanto como cada estação de trabalho na rede pode transmitir dados, desde que outra não esteja transmitindo ao mesmo tempo, este tipo de rede tende a ficar menos produtiva apesar de ter boa segurança e simplicidade para seu crescimento. Afinal, basta conectar o cabo a uma nova estação.

A topologia em anel é, na verdade, uma topologia ponto a ponto em que todos os equipamentos estão interligados entre si, em um circuito fechado, como pode-se observar na Figura 2.5.



Topologia em anel

Figura 2.5 – Topologia em Anel.

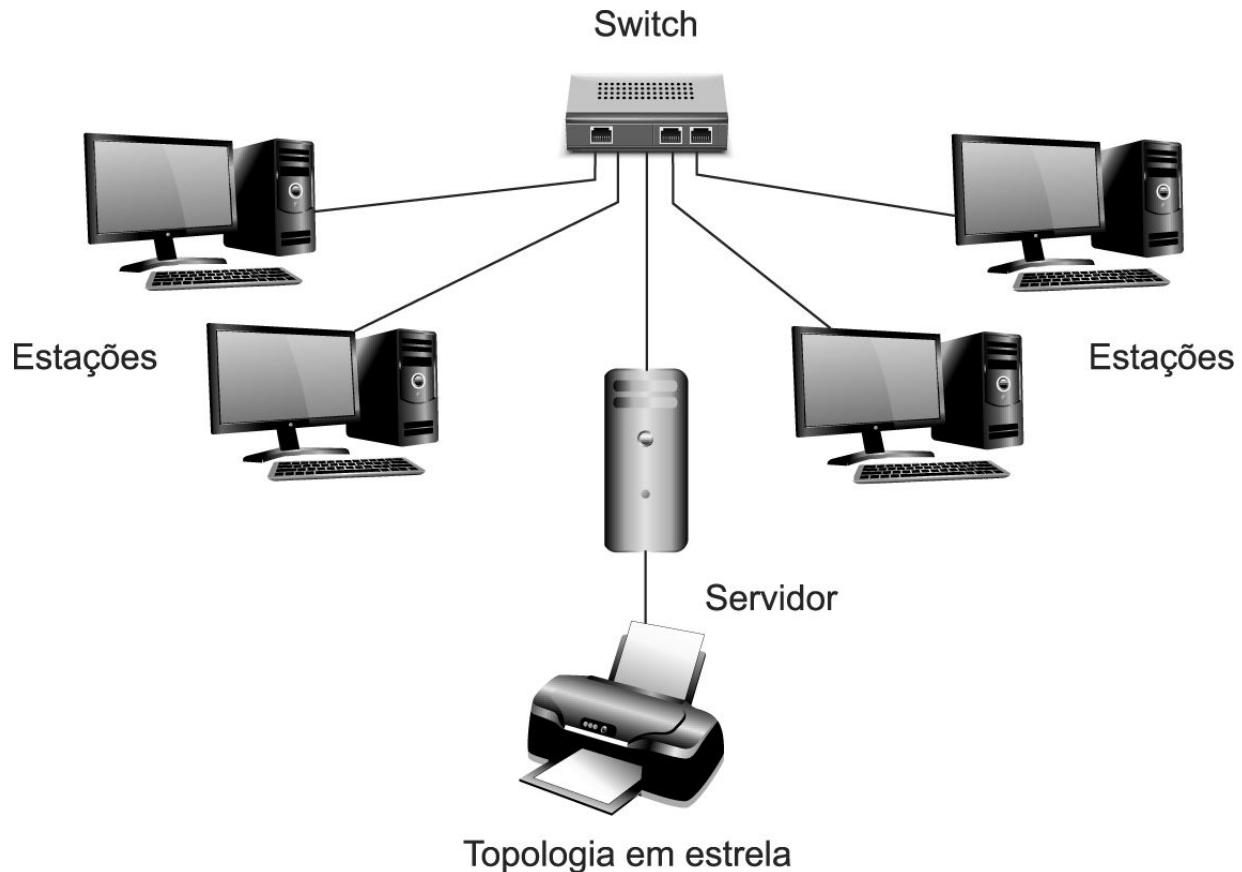


Figura 2.6 – Topologia Estrela.

Uma rede em anel é composta por computadores e dispositivos conectados por meio de um caminho fechado.

Nesta configuração, as estações remotas conectadas ao anel podem não se comunicar necessária e diretamente com um computador central.

Esta configuração exige que cada estação tenha capacidade de seletivamente mover mensagens da rede e passá-las para o próximo nó da rede, ou seja, o próximo dispositivo neste anel.

Elas utilizam em geral ligações ponto a ponto e estas ligações atuam com um único sentido de transmissão de pacotes de rede. O pacote de dados circula no anel do computador que enviou o pacote até chegar ao computador destino.

Neste tipo de rede se um dos nós da rede, um computador, falhar pode ocorrer falha em toda a rede.

E finalmente a topologia em estrela, que é onde os computadores estão conectados por meio de um computador central.

Neste tipo de rede, se um computador falhar, somente ele será afetado. Os demais continuarão operando na rede normalmente.

Entretanto, nesta topologia, caso o computador central tenha uma falha, toda a rede irá parar.

Estudaremos a seguir a topologia que mais nos interessa no que diz respeito à segurança da informação: a topologia chamada de Backbone (espinha dorsal), que em algum momento você já deve ter ouvido alguém falar: "... ahh por que o nosso backbone deu problema..."

2.2.5.1 Backbones

Uma rede muito complexa, como a de uma grande escola técnica ou de uma grande empresa, necessita de um modo inteligente de identificar os elementos constituintes dessa rede para efeitos de manutenção, ampliação etc. Para isso há a rede segmentada em partes menores.

Estes segmentos podem apresentar topologias diferentes, mas a comunicação ocorrerá como se existisse uma única topologia.

O backbone é, então, a parte da rede na qual todos os segmentos e servidores se ligam.

Uma rede necessariamente tem somente um servidor. Normalmente existe um conjunto de servidores, sendo cada um para uma função ou conjunto de funções.

Todos os chamados segmentos de rede e servidores ligam-se diretamente ao backbone de modo que qualquer segmento esteja somente a distância do segmento dos servidores daquele backbone.

Como os segmentos estão próximos dos servidores, isso torna a rede muito mais eficiente. Um segmento é o termo generalista para qualquer seção da rede que não faça parte do backbone, somente os servidores ligam-se diretamente ao backbone, todos os outros dispositivos se ligam a um segmento de rede.

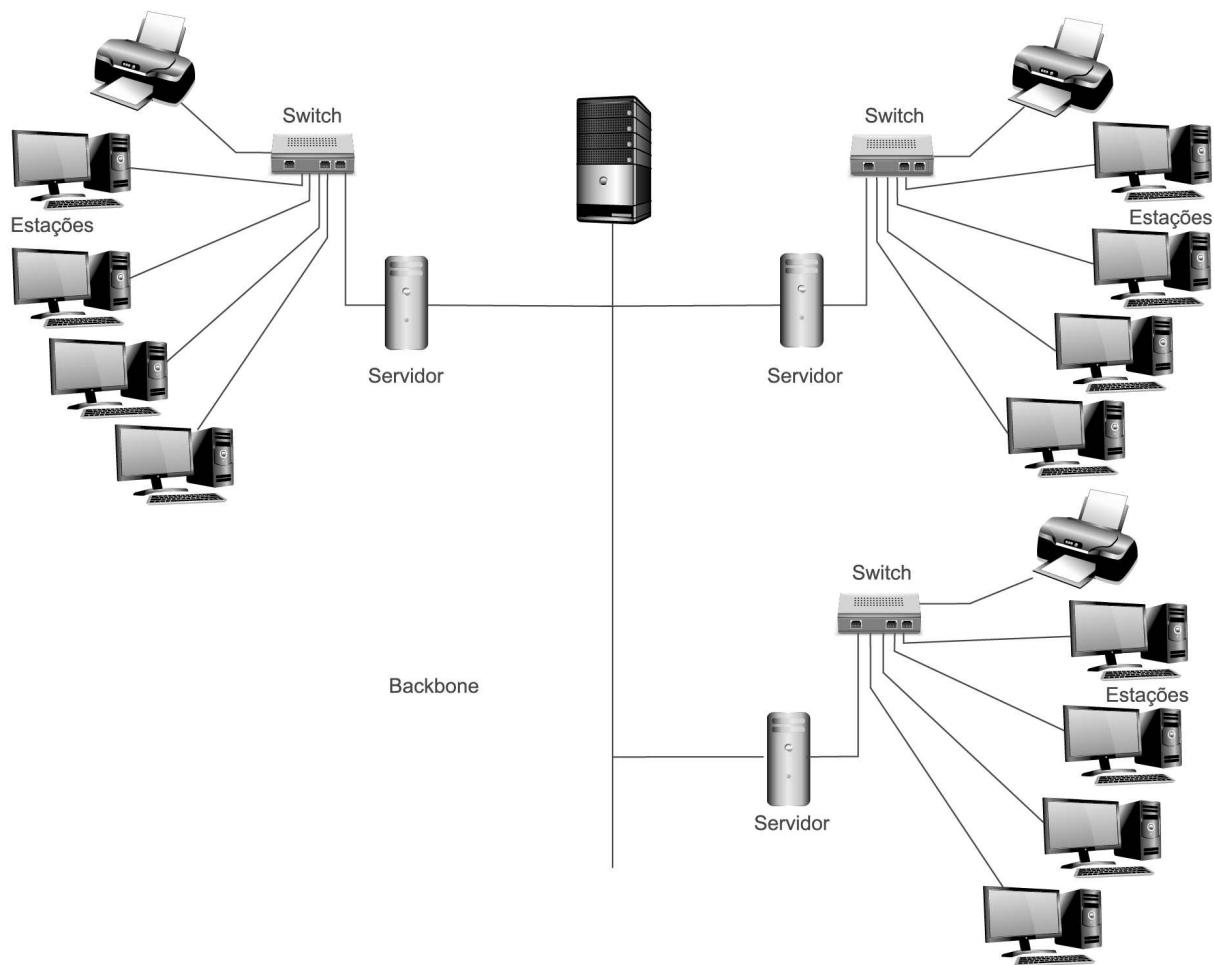


Figura 2.7 – Backbone.

2.2.5.2 Pacotes de dados

Em uma rede de computadores a estrutura unitária de transmissão de dados chama-se **pacote** ou **datagrama**, que nada mais é que uma sequência de dados transmitida.

A informação que se quer transmitir normalmente é quebrada em inúmeros pacotes e então transmitida.

Além das partes componentes da informação, um pacote de dados possui um cabeçalho, que contém informações importantes para a transmissão, como o endereço do destino, somatórios para checagem de erros, prioridades, entre outras.

Amplie seus conhecimentos

Não abordaremos os demais equipamentos que fisicamente compõem um rede, pois não é este o objetivo deste livro. Mas você, leitor, pode pesquisar e criar um diagrama (desenho) com todos os componentes físicos e servidores que uma rede pode ter.

Pesquise sobre a existência de servidores de e-mail, servidor de banco de dados, servidor de impressão, servidor de web, modems ADSL, roteadores, wireless etc.

2.2.5.3 Conectando à Internet

Agora só falta mostrarmos como um computador em rede se conecta à internet e como uma página que está em um servidor do outro lado do mundo chega até você. Em outras palavras, como uma cracker se conecta e tem acesso a outro computador.

Como já sabemos o que é um servidor DNS e um protocolo TCP/IP, estudaremos, mais detalhadamente, como se dá o funcionamento da internet.

Como um site hospedado em um servidor na Europa pode chegar até nossos computadores em questão de segundos? Como isso funciona? Quais os caminhos usados?

A estrutura é basicamente a mesma sempre. Um computador isolado, ou uma rede de computadores, se conecta a um provedor de acesso (hoje em dia praticamente 99% em banda larga) e a rede

desse provedor se conecta a um dos backbones disponíveis no país.

Backbones? Sim, eles estão presentes aqui outra vez.

Antes, ilustraremos, a seguir, a conexão de seu computador até a página de internet que está em algum lugar do mundo, para iniciar sua visualização do todo:



Figura 2.8 – Conexão a Web.

Chamamos atenção, na figura, para a linha que representa a ligação e o tráfego de informações entre os pontos. Ela engrossa à medida que se afasta da sua máquina/rede.

Buscamos representar porque a largura de banda (ou seja, a velocidade de internet) é muito maior nos backbones e nos provedores do que numa rede doméstica ou no trabalho.

Se você acha sua banda larga rápida é porque nunca deve ter experimentado a velocidade das instalações de um provedor ou até mesmo de um backbone!

Sabemos que existem backbones nacionais em cada país. Ou seja, as portas de entrada para a conexão de internet em um país.

O sinal, ou melhor, os dados e o tráfego de informações costumam chegar até eles por meio de satélite ou cabos submarinos de fibra ótica de altíssima velocidade.

Agora ilustraremos, para visualizarmos melhor, como a página de um site que você digitou no seu navegador chega até você.

Antes devemos lembrar que o endereço de um determinado site (por exemplo, “google.com.br”) é uma forma traduzida de uma sequência de números.

Esses números, conhecidos como IP, identificam cada máquina que tem acesso à internet, seja ela doméstica ou um servidor onde estão hospedados centenas de sites.

Os IPs são únicos, algo como as impressões digitais dos seres humanos. Cada máquina conectada à internet possui um IP. Portanto, nenhuma outra máquina tem o número de identificação de outra.

Ao ligar o computador e iniciar a conexão com a internet, o provedor fornece um IP para identificar a máquina na rede mundial de computadores.

O provedor é o dono de uma determinada faixa de endereços IP e disponibiliza um deles temporariamente para que se dê a navegação na web.

Na Figura 2.9, é possível observar um exemplo visual sobre como acontece o primeiro passo da sua conexão com a internet. Note o número 192.168.25.194 – isso é um IP, número com o qual as máquinas são identificadas em nível mundial.

Pronto, já estamos conectados ao provedor de acesso, mas os sites que existem no mundo não estão todos dentro da rede deste provedor no qual nos conectamos.

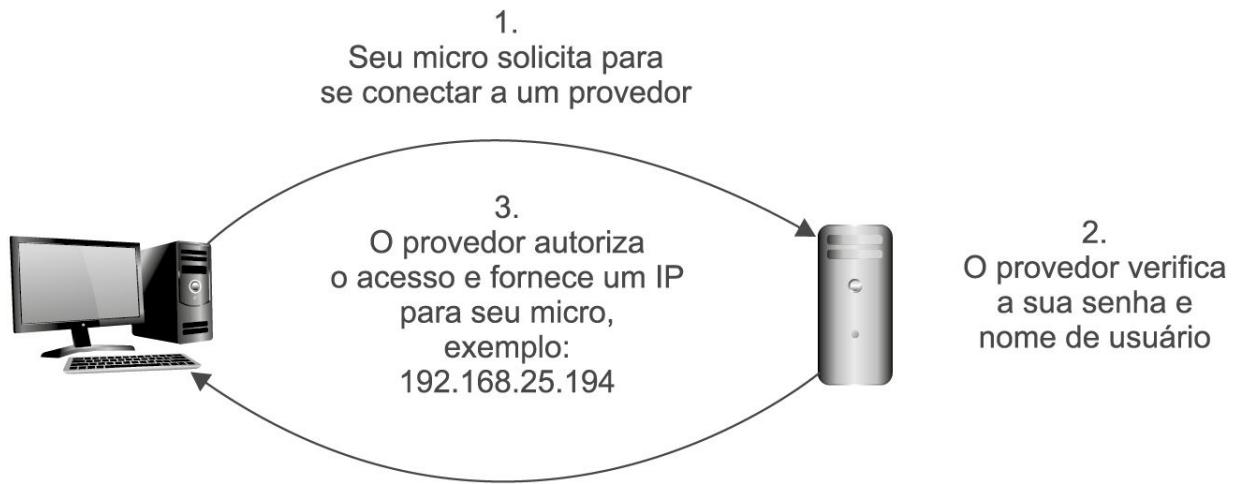


Figura 2.9 – Solicitação de acesso.

Supondo então que desejamos acessar um site, por exemplo, nos Estados Unidos.

Agora vamos perceber que entra em cena um personagem que já estudamos, o servidor de DNS, e outro também importante nas redes e na internet, que é o roteador.

O servidor de DNS é o responsável por “traduzir” o endereço de um site para o número IP (ou vice-versa), que informa em que computador aquele site está armazenado.

Fique de olho!

Lembrando que se isso não fosse como acabamos de apresentar, você não digitaria “www.google.com.br” em seu navegador, mas sim 173.194.73.147. Experimente, por exemplo, digitar esse IP na barra de endereços do seu navegador e veja que em segundos você estará na página da referida empresa.

Agora imagine ter que decorar os endereços de todos os sites que você mais gosta? Seria extremamente incômodo, chato e confuso. Ainda bem que existe o DNS. Com ele não precisamos digitar 31.13.85.8 toda vez que formos acessar o Facebook!

Ao digitarmos um endereço no navegador e apertarmos a tecla “enter”, ele envia um pacote de dados para o provedor com o endereço do site que desejamos acessar e o endereço de IP da máquina utilizada.

O servidor de DNS, então, tem acesso a esse pacote e o analisa. Ao fazer isso, ele traduz o endereço do site para um IP e se comunica com o roteador para encontrar o endereço de IP.

O roteador pega o endereço de IP e verifica se está dentro da rede do provedor ou não. Caso não esteja, ele envia o IP para outro roteador fora da rede do provedor. Assim o pedido de acesso ao site passa de roteador em roteador, mundo afora, até encontrar a máquina que possui o IP 31.13.85.8.

Ao chegar ao servidor onde o site está armazenado, o pacote é processado e reenviado para o IP de origem dele, ou seja, o IP da sua máquina.

Ele refaz todo o caminho, entra na rede do provedor e, então, chega à máquina utilizada, trazendo junto com ele a página cujo acesso foi solicitado.

Vejamos, na Figura 2.10, como se dá passo a passo esse processo:

Passo 1: Temos o seu computador (vamos imaginar então que você quisesse acessar o Facebook).

Passo 2: A figura mostra a rede do seu provedor de acesso, onde seu pedido de acesso ao Facebook chega e é traduzido pelo servidor de DNS para o número do IP da máquina onde está o Facebook (no caso, 31.13.85.8).

O servidor de DNS encaminha seu pedido para o roteador, que analisa a informação e envia para o passo 3, o Backbone Brasil.

Passo 3: O backbone brasileiro analisa o pacote e o envia para os roteadores de fora do país (4), pois o IP que consta no seu pedido não é brasileiro e ele já tem uma rota para o seu pacote.

Passo 4: Os roteadores direcionam seu pedido para um backbone norte-americano (5).

Passo 5: O backbone norte-americano verifica a informação e direciona o pedido para outro roteador, que, por sua vez, leva sua solicitação de dados até o servidor que possui o IP 31.13.85.8.

Passo 6: Seu pedido é analisado e mandado de volta para o IP de origem – no caso, o do seu micro –, levando junto a informação solicitada. O pacote refaz o caminho e assim o site aparece em seu monitor.

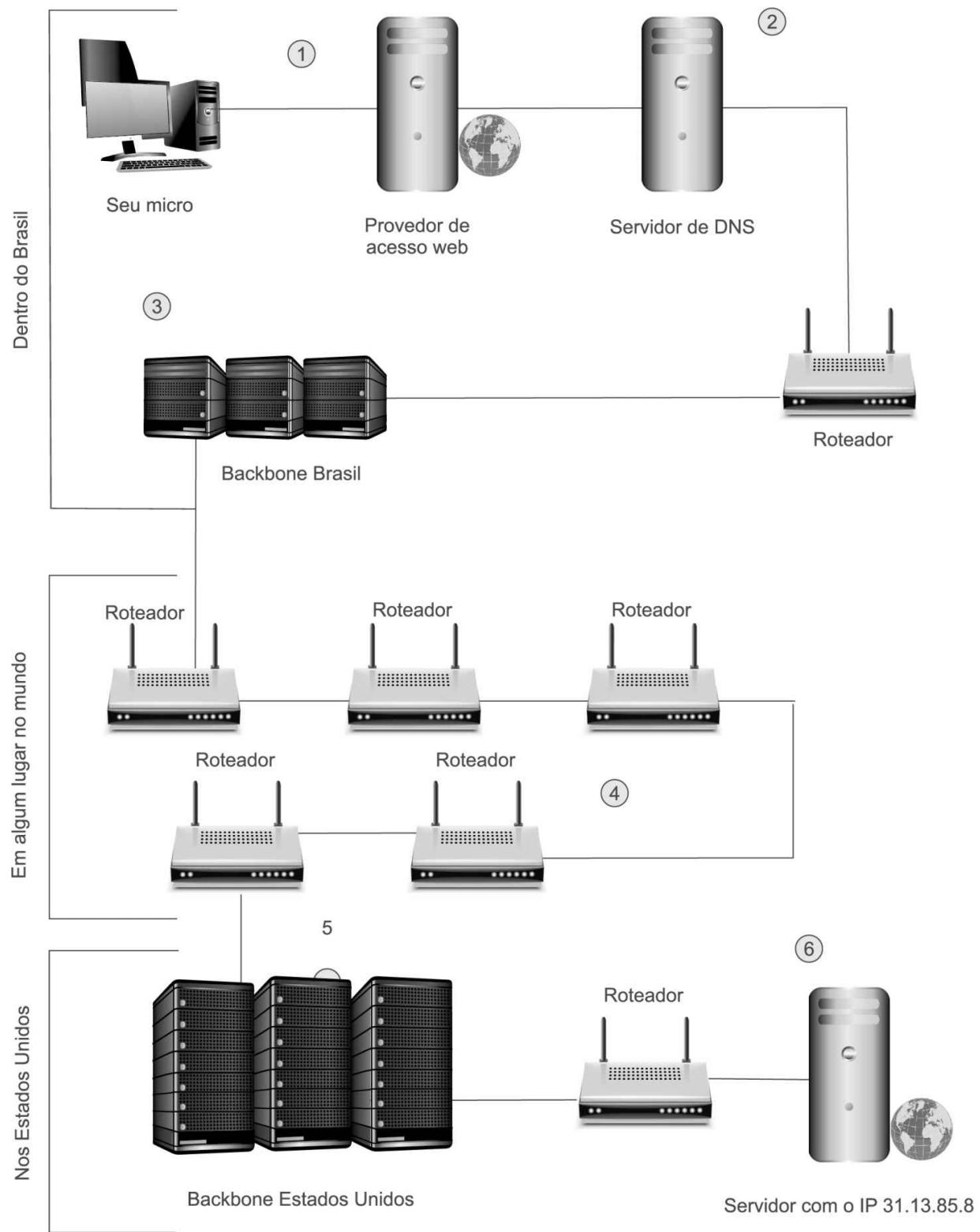


Figura 2.10 – Acesso a um site na internet.

Essa é uma explicação bem simples sobre como funciona a navegação na internet, desde o momento em que nos conectamos a uma rede até a exibição de um site desejado no monitor.

Amplie seus conhecimentos

Existem programas que traçam a rota de um pacote de dados desde a sua máquina até um endereço de IP ou um site. Esses programas são conhecidos como Tracerouters. Há programas que exibem até um mapa do mundo indicando cada cidade onde seu pacote de dados esteve. Pesquise por “visual traceroute” no Google e descubra mais.

Para brincar de descobrir o IP referente ao endereço de um site, basta experimentar usar um serviço conhecido como “Whois”, no endereço: <http://www.whois.net/>.

Vamos recapitular?

Neste Capítulo 2, aprendemos o que é uma rede, como os computadores se comunicam em rede e como são identificados na internet. Além disso, aprendemos como funciona uma conexão a internet. Já tem uma visão do mundo onde os Hackers navegam, e como é este mundo de informações que você vai se preocupar em manter a segurança.

No próximo capítulo, conheceremos mais detalhadamente os princípios da segurança da informação, agora que já conhecemos os ambientes de redes.



Agora é com você!

- 1) Para que o seu computador seja encontrado e possa fazer parte da rede mundial de computadores, ele necessita de um endereço único. Explique o que é este endereço único e como ele é controlado:
- 2) No número IP 192.168.25.194, o valor 192 identifica o quê?
- 3) Pesquise e responda a seguinte questão: se o servidor de DNS é o responsável por “traduzir” o endereço de um site para o número IP, quem traduz um número IP para o nome de um site?

- 4) Quais são os principais objetivos de uma rede? Cite e explique 3 (três).
- 5) TCP/IP é um protocolo ou um formato de endereço para a internet ou uma rede? Explique.
- 6) Em uma rede cliente-servidor existem dois tipos de computadores. Como eles são chamados?

3

Princípios da Segurança da Informação

 Para começar

Como já aprendemos os conceitos gerais sobre a segurança da informação, neste capítulo vamos explorar e conhecer mais detalhadamente os princípios básicos da garantia desta segurança e quando ocorrem as violações destes princípios. Vamos estudar também as vulnerabilidades que podem e devem ser combatidas para a manutenção dos princípios, e o que são e como atuam as políticas de segurança da informação na garantia também destes princípios.

São três os princípios que orientam e sustentam a segurança da informação, quais sejam:

- 1) Integridade;
- 2) Confidencialidade;
- 3) Disponibilidade.

3.1 Princípio da integridade de informação

O primeiro dos três princípios da segurança da informação que estudaremos é a integridade.

É ela que garantirá que a informação não será alterada de forma não autorizada. Portanto, é íntegra, mas com um detalhe a ser considerado: íntegra não significa exata. Ou seja, com uma informação podemos ter integridade, mas não exatidão. Por outro lado, não podemos ter exatidão sem integridade.

O controle da integridade deve proteger a informação de ameaças involuntárias ou intencionais, controlando os direitos de acesso, bloqueando os acessos indevidos de pessoas não autorizadas.



Figura 3.1 – Integridade 1.

Para considerarmos uma informação íntegra, ela não pode ter sido alterada de forma indevida ou não autorizada. Por exemplo, o valor de seu salário bruto no sistema de folha de pagamento com valor diferente e menor do que o do mês passado. Neste caso, ele pode ter sido alterado por erro de operação (manutenção indevida de dados) ou por um funcionário mal-intencionado que modificou os valores nos bancos de dados da empresa.

A integridade da informação é fundamental para os negócios da empresa e para a comunicação interna ou com outras empresas.

Quem recebe uma informação necessita ter a segurança de que a informação recebida, lida ou ouvida é exatamente a mesma que foi colocada à sua disposição por quem a emitiu para esta

finalidade.

Ser íntegra significa estar em seu estado original, sem ter sofrido qualquer alteração por alguém não autorizado. Se uma informação sofre alterações em sua versão original, ela perde sua integridade, levando a erros e fraudes, prejudicando a comunicação e os processos de decisão de uma empresa como um todo. Isto não significa que uma informação original não possa ser alterada, mas que qualquer alteração só pode ser feita por pessoa autorizada, ou seja, com direito de acesso e alteração de uma informação.

A perda de integridade ocorre quando uma informação é corrompida, falsificada, indevidamente alterada, ou excluída. Por exemplo, você acessa seu banco pela internet e seu saldo aparece zerado, sem que tenha ocorrido nenhuma movimentação da conta, ou simplesmente sua conta desapareceu e você recebe uma mensagem de que a conta não existe ou é inválida. Isso seria um caso de perda de integridade.

Uma informação poderá ser alterada de várias formas, tanto em seu conteúdo quanto no ambiente que lhe oferece suporte, isto é, o ambiente onde se encontra armazenada. Desta forma, a perda de integridade de uma informação poderá ocorrer sob duas formas:

- » Alterações do conteúdo dos dados;
- » Quando forem realizadas inclusões, alterações ou exclusões de parte de seu conteúdo;
- » Alterações no ambiente que oferece suporte ou armazena a informação.



Gst/Shutterstock.com

Figura 3.2 – Acesso aberto à informação.

Isto acontece quando são realizadas alterações na estrutura física e/ou lógica onde a informação está armazenada, seja nos sistemas e programas que apresentam a informação, seja nas estruturas de bancos de dados que armazenam estes dados.

Para garantirmos a integridade das informações temos de assegurar que apenas as pessoas ou sistemas autorizados possam fazer alterações na forma e no conteúdo de uma informação ou que alterações causadas por acidentes ou defeitos de tecnologia não

aconteçam também no ambiente de hardware (computadores, servidores, meios magnéticos de armazenagem) e comunicações (redes) no qual ela é armazenada e pela qual transita.

Em síntese, integridade significa que nos dados originais nada foi acrescentado, retirado ou modificado.

A integridade de informações também diz respeito ao nível de confiança das informações do banco de dados, ou seja, a credibilidade e a lógica das informações.

Regras de restrição de integridade configuram um banco de dados a ser alimentado por informações com características lógicas específicas, validadas antes do seu armazenamento, diminuindo a probabilidade de falta de integridade no banco de dados. Estes aspectos são tratados no projeto e modelagem de dados em um processo de desenvolvimento de sistema de informações.

Para revermos o que é a quebra de integridade, citamos:

- » Um funcionário que modifica o valor do seu salário sem autorização no sistema de RH;
- » Um vírus modifica arquivos em um computador;
- » Hackers modificam um site.

Estes são alguns exemplos simples de quebra de integridade de informação.

Mais adiante você conhecerá mecanismos de controle para a garantia da integridade das informações.

Temos de considerar que hardware, software e os mecanismos de comunicação devem trabalhar de forma conjunta para manter e processar dados corretamente, assim como mover os dados para os destinos previstos, sem nenhuma alteração não prevista.

Como princípio, os sistemas operacionais de computadores e as redes devem ser protegidos contra interferências e contaminações do ambiente exterior.

Para assegurar que atacantes externos ou erros cometidos por usuários não comprometam a integridade dos sistemas ou dados, todos os ambientes computacionais devem fornecer mecanismos de controle de segurança.

Os usuários geralmente afetam um sistema ou a integridade de seus dados por engano e não intencionalmente, embora usuários internos de uma empresa também possam realizar atos mal-intencionados.

Programas de sistemas devem fornecer mecanismos que verifiquem os valores de entrada, se os mesmos são válidos e razoáveis. Isto é parte das obrigações dos programadores e analista de sistemas em relação à integridade da informação.

Os bancos de dados devem deixar apenas que indivíduos autorizados possam modificar dados, e os dados em trânsito devem ser protegidos por criptografia ou outros mecanismos que garantam o não acesso, ou modificação, deles sem autorização.

Fique de olho!

Mais à frente, falaremos mais sobre criptografia.

Quando um ataque externo inserir um vírus, uma bomba lógica, ou um programa backdoor (estudaremos adiante em detalhes) em um sistema, a integridade dos dados e informações de um sistema é comprometida.

Inserção e alteração de dados com erros por parte de um usuário também comprometem uma informação em sua integridade, lembrando que as informações se propagam rapidamente em um ambiente computacional, assim como os erros, tornando-se alto o custo para corrigi-los.

3.2 Princípio da confidencialidade de informação

Nem todas as informações são sigilosas, ainda que sejam informações importantes, consideradas críticas.

Algumas informações ou dados necessitam de confidencialidade ou sigilo, entre elas:

- 1) dados pessoais (por exemplo, número de telefone, endereço, CPF e RG, senha de acesso a bancos ou outros sites comerciais);
- 2) dados de cartões de crédito (por exemplo, número do cartão, código de segurança, senha);
- 3) dados de fornecedores ou de clientes de uma empresa;
- 4) dados de políticas financeiras de uma organização, ou de uma pessoa, como seu saldo bancário; e
- 5) dados de marketing, ou política de preços de uma empresa, ou seus dados de rendimentos pessoais mensais, anuais etc.

A perda desta confidencialidade provoca custos e prejuízos a empresas e pessoas, como perdas de clientes e fornecedores, perda de vendas e faturamento, perdas na imagem pública de uma empresa ou pessoa.



Ducu59us/Shutterstock.com

Figura 3.3 – Confidencialidade e privacidade.

O princípio de manutenção da confidencialidade deve ser dirigido para o direito das pessoas e empresas e na classificação dos dados e informações.

O princípio da confidencialidade da informação tem como objetivo garantir que apenas a pessoa certa tenha acesso à informação devida para ela, ou seja, informação correta para a pessoa correta.

Ampliando nossos conceitos podemos afirmar que as informações trocadas entre pessoas e empresas normalmente não deverão ser do conhecimento de todos que fazem parte de uma empresa.

Muitas das informações geradas por algumas pessoas se destinam a um grupo específico de pessoas em uma empresa ou de sua rede de amigos e, muitas vezes, a uma única pessoa. Isso significa que esses dados deverão ser acessados e conhecidos apenas por um grupo limitado de pessoas, que deve ser definido pela pessoa ou, no caso de uma empresa, por um responsável pelas informações.

As informações devem possuir um grau de confidencialidade para cada uma, que deverá ser mantido para impedir que as pessoas não autorizadas tenham acesso a ela.

3.2.1 Engenharia social

Você conhecerá agora um pouco sobre engenharia social.

A engenharia social é enganar outra pessoa para obter o compartilhamento de informações confidenciais, colocando-se como uma pessoa autorizada a acessar essas informações.

Alguns usuários podem intencionalmente ou accidentalmente revelar informações sigilosas por não criptografá-las antes de enviá-las a outras pessoas. Eles podem, ainda, ser vítimas de um ataque de engenharia social, que se caracteriza pelo compartilhamento de segredos comerciais de uma empresa, pela falta dos cuidados necessários na proteção de informações confidenciais quando estas são processadas por sistemas, ou pelo envio de mensagens de sistemas via e-mails automáticos.

A confidencialidade pode ser fornecida por meio da criptografia de dados, uma vez armazenados e transmitidos durante o tráfego em rede, de um rigoroso controle de acesso aos dados, de uma rigorosa classificação de dados sigilosos ou não e principalmente de treinamento de pessoal nas empresas, sobre quais são os procedimentos adequados com a informação.

Quando falamos em tráfego de rede, queremos dizer que ter confidencialidade na comunicação é ter a segurança de que o que foi enviado a alguém ou escrito em algum lugar (um e-mail, por exemplo) só será acessado ou lido por quem tiver autorização para tal.

Fique de olho!

Pensemos no caso de um cartão de crédito. O número do cartão só deverá ser conhecido por seu proprietário e pela loja onde é usado no momento da compra. Se esse número for descoberto por alguém mal-intencionado, como nos casos noticiados sobre crimes da internet, o prejuízo causado pela perda desta confidencialidade poderá ser muito alto. Esse número poderá ser usado por alguém para fazer compras na internet ou em qualquer estabelecimento que receba pagamentos com cartão de crédito, trazendo prejuízos financeiros e uma grande dor de cabeça para o proprietário do cartão, além de afetar a imagem da empresa que recebeu pagamento com estes cartões.



Exemplo

Jantávamos eu e um colega, mestre e escritor, ainda no tempo em que se passava o cartão de crédito em uma maquininha com carbono, como ocorria antigamente. Já naquela época, o atendente do restaurante fez duas cópias dos dados do cartão, fazendo com que no extrato de meu colega constasse duas vezes cobrança no mesmo estabelecimento com valores inclusive diferentes.

Hoje em dia isso é mais fácil ainda de ocorrer, se você falar ou mostrar algum papel com a senha de seu cartão de crédito, ou os sistemas do estabelecimento que guardam e transmitem os dados do cartão para a operadora forem atacados e estes dados confidenciais, copiados.

Isto é perda de confidencialidade e uma grave falha em segurança da informação.

Manter a confidencialidade é um dos fatos mais determinantes para a segurança e uma das tarefas mais difíceis de implementar, pois envolverá todos os elementos que compõem a comunicação de informações, desde quem a emite, passando pelo caminho percorrido, até quem a recebe.

Além disso, as informações têm diferentes graus de confidencialidade, normalmente associados a seus valores sociais ou empresariais.

Quanto maior for o grau de confidencialidade de uma informação, maior será o nível de segurança necessário na estrutura tecnológica e humana que participar destes processos: utilização, acesso, trânsito e armazenamento das informações.

3.2.2 Grau de confidencialidade

As informações geradas pelas pessoas tanto no ambiente pessoal quanto em uma empresa têm uma finalidade específica e destinam-se a um indivíduo ou grupo de indivíduos dentro da empresa.

Portanto, é necessário a existência de uma classificação com relação à sua confidencialidade.

É o que chamamos de grau de sigilo, isto é, a graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem as permissões de acesso a esta mesma informação.

O grau de confidencialidade é um dos componentes mais importantes no processo de classificação da informação.

Normalmente as informações possuem os seguintes tipos de classificação quanto à confidencialidade:

- » Confidencial.
- » Restrito.
- » Sigiloso.
- » Público.

Dizem que o único computador totalmente seguro é aquele desligado da tomada. A arte da engenharia social concentra-se no elo mais fraco da corrente da segurança de computadores: os seres humanos. Logo o aspecto acesso à informação, mesmo aquelas com nível de classificação de confidencialidade mais alto, pode ser obtido por meio de pessoas ou ingênuas ou mal-intencionadas.

Como um ataque da chamada “engenharia social” pode revelar muitas informações, como tornar um sistema de computadores mais seguro?

A resposta é educação e difusão da classificação da informação, explicando aos empregados e pessoas ligadas direta ou indiretamente a um determinado sistema a importância de uma política de segurança e confidencialidade. Assim evitar-se-á o ataque de pessoas que poderão tentar manipulá-los para ganhar acesso a informações privadas.

Podemos dizer e afirmar que este é um excelente começo para tornar segura sua rede ou sistema de informações.

O controle de acessos será alvo de nossos estudos nos próximos capítulos deste livro, quando veremos características de uma política de segurança.

Analisaremos políticas de controle de acessos a arquivos de senhas, programas fonte de sistemas, arquivos de dados, arquivos de log (registro de transações em bancos de dados), programas utilitários e sistema operacional de computadores e redes.

Amplie seus conhecimentos

Existem casos de pessoas que ligam para o provedor de acesso à internet e perguntam: "Por favor, perdi minha senha de internet. Poderia olhá-la para mim?" Alguns provedores pedem documentação para comprovar que é o dono da conta, outros (funcionários insatisfeitos em sua maioria) não ligam e passam até o número do cartão de crédito de algum usuário se lhe pedirem. Esse método é utilizado também para conseguir informações sobre uma pessoa em especial.

Vá a uma companhia telefônica e peça a segunda via de uma conta de telefone qualquer. Na maioria das vezes não lhe pedem documento e você consegue o endereço residencial de qualquer pessoa. Alguns filmes como *Hackers* e *Caçada Virtual* mostram bastante essa técnica.

3.3 Princípio da disponibilidade de informação

Toda e qualquer informação deve estar disponível sempre que for necessário. Deriva deste princípio a ideia de que devemos ter “a informação certa, na hora certa para a pessoa certa”, o que une os três princípios da segurança da informação.

Os recursos tecnológicos da informação devem ser mantidos sempre em bom funcionamento e devem ser capazes de ser recuperados de forma rápida e completa, em casos de desastres naturais ou acidentais.

O caso citado neste livro sobre ataque DDoS ao site da Origin®, que o tornou indisponível, caracteriza perfeitamente bem uma quebra da disponibilidade da informação.

A disponibilidade da informação se refere a toda estrutura física e tecnológica necessária para permitir o acesso, o tráfego e o armazenamento das informações e dados.

Por exemplo, se durante uma reunião de diretoria de uma empresa os serviços de banco de dados falham, e com isso impede que seja tomada uma determinada decisão em pauta, estaremos com uma quebra de disponibilidade também.

Se você acessa seu banco pela internet para saber seu saldo antes de emitir um cheque, por exemplo, e o site de seu banco está fora do ar, ou sobrecarregado e não responde, isto também caracteriza uma indisponibilidade de informação. Ou seja, a quebra do princípio que estamos discutindo.

Para proteger a disponibilidade da informação, é necessário saber quem são seus usuários e organizar e definir, para cada caso, as formas de disponibilização da informação. Em outras palavras,

quem tem acesso e uso para quando for necessário.

A disponibilidade da informação é sempre considerada com base no valor que esta informação tem e no impacto da indisponibilidade dela. Sites de internet, em particular, têm a necessidade de garantir de maneira ininterrupta o acesso e a disponibilidade de informações e recursos.

Podemos considerar então a existência da preocupação com a proteção da informação na internet, pois o avanço tecnológico traz consigo o surgimento de novos métodos de ataques de hackers atrelado a uma maior vulnerabilidade de sistemas que não se atualizam no mesmo ritmo.

Logo, manter disponibilidade é um princípio, porém é mais um ponto da segurança que deve ser sempre considerado.

É necessário que haja sempre controle sobre pontos específicos de falhas que devem estar em vigor, caso as medidas necessárias de backup tenham de ser tomadas. Outrossim, mecanismos de redundância de dados (bancos de dados espelhados) devem estar no local quando necessário. Desta forma, os efeitos negativos de componentes ambientais que geram indisponibilidade de informação poderão ser evitados. Por exemplo, um servidor de banco de dados parar por falha de hardware, como queima do equipamento por sobrecarga elétrica, deixaria indisponíveis todas as suas informações.

Uma medida de segurança seria o backup frequente dos bancos de dados para recuperação em outro equipamento, ou então a existência de um equipamento sobressalente, em que estariam duplicadas todas as informações. Este equipamento redundante substituiria automaticamente o equipamento queimado ou interrompido.

A disponibilidade de informações pode ser afetada por falha de hardware ou por falha de software, por isso a importância de backups para permitir a recuperação e a continuidade da disponibilização das informações.

Observe que as questões ambientais como calor, frio, umidade, eletricidade estática, bem como a contaminação por vírus ou ataques, também podem afetar a disponibilidade de um sistema de informações.

Então o princípio da disponibilidade deve impedir a interrupção dos serviços e produtividade com sistemas de informação.

3.3.1 Vulnerabilidades

As vulnerabilidades são os pontos que, ao serem explorados por pessoas mal-intencionadas, afetam a confidencialidade, a disponibilidade e a integridade das informações de um indivíduo ou empresa.

Um dos primeiros passos para a implementação da segurança é rastrear e eliminar os pontos vulneráveis de um ambiente de tecnologia da informação.

Muitas vezes as palavras ameaça, vulnerabilidade, exposição e risco são usadas para representar a mesma coisa, apesar de terem diferentes significados e relações entre si.

É importante compreender a definição de cada uma delas, mas o mais importante é que você compreenda a associação de uma às outras.

Vulnerabilidade pode ser um software, hardware ou falha de um processo que pode fornecer a um atacante uma porta aberta que ele está à procura, para entrar em um computador ou rede e ter acesso não autorizado aos recursos dentro deste ambiente.

Uma ameaça é qualquer perigo potencial para a manutenção dos princípios da segurança da informação.

Um agente de ameaça pode ser um intruso que venha a acessar uma rede por meio de uma porta no firewall (mais adiante, veremos em detalhes o que é um firewall), um determinado processo de sistemas acessando de forma que viole as políticas de segurança, um furacão (tempestade) destruindo uma instalação de um centro de processamento de dados, ou um empregado que venha a cometer um erro não intencional que poderia expor informações confidenciais ou então destruir a integridade dos dados de um arquivo.

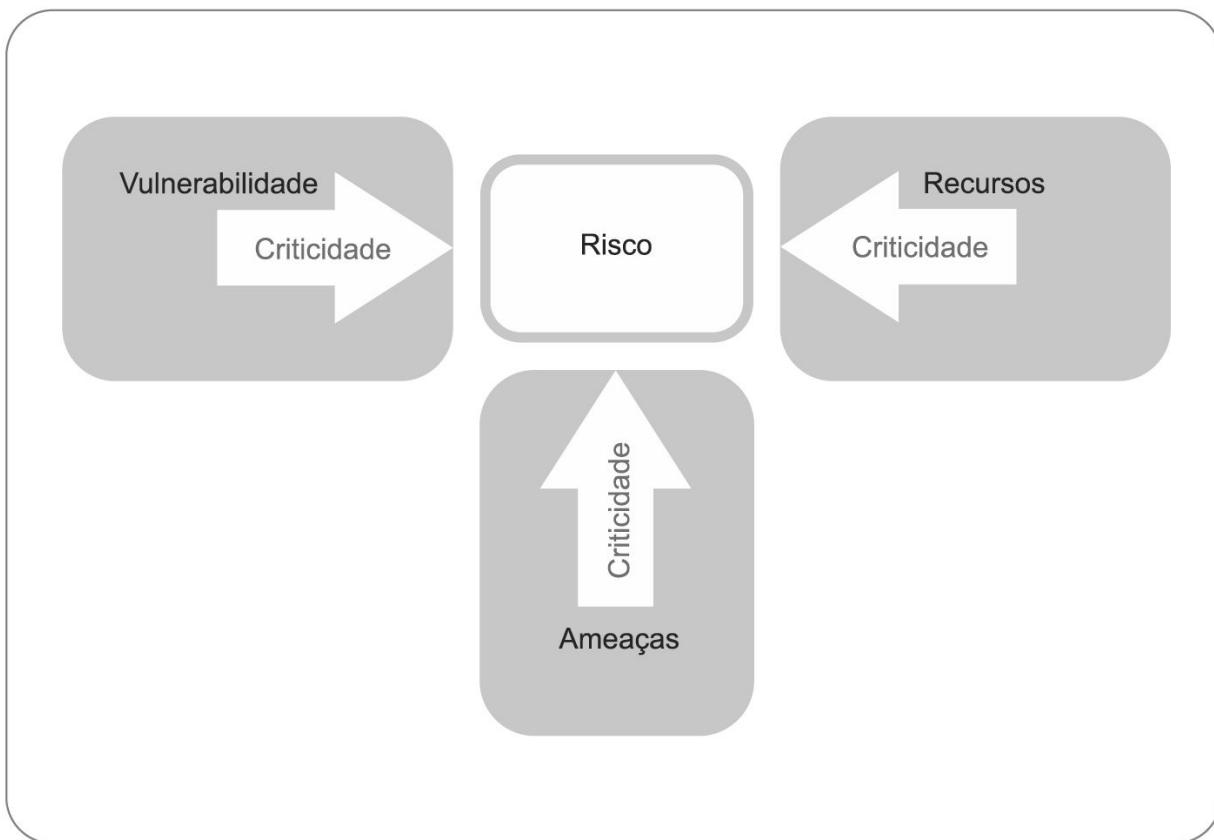


Figura 3.4 – Ameaças e Riscos.

A exposição é o fato de as informações e sistemas de tecnologia da informação serem expostos a perdas a partir de um agente de ameaça interna ou externa.

Uma vulnerabilidade pode causar danos e perdas a uma organização, se exposta a possíveis danos por esta exposição.

Por exemplo, se o gerenciamento de senhas é frouxo e as regras de senha não são aplicadas ou não existem, a empresa pode ter suas senhas de usuários expostas, capturadas e utilizadas de forma distinta de seu titular, com finalidades destrutivas ou de violação de confidencialidade.

É muito normal em empresas existirem regras para as senhas de acesso a rede e banco de dados com no mínimo oito caracteres, sendo obrigatório que um deles seja numérico. Além disso, elas não podem conter nome, sobrenome ou data de nascimento, e o usuário é obrigado a trocá-las com uma frequência determinada.

Hoje, até mesmo alguns bancos solicitam que seus clientes troquem de senha com frequência. Do contrário, informam, por exemplo, que a senha não é trocada há mais de seis meses.

Na prática, alguém do RH utiliza uma senha simples para usuário. Outra pessoa mal-intencionada pode copiá-la a fim de ter acesso aos salários de outros funcionários, mesmo que seja somente para consulta.

Contramedida, ou salvaguarda, é o que atenua um risco potencial.

Uma medida preventiva é uma configuração de software, hardware ou um procedimento que elimina uma vulnerabilidade dos sistemas ou reduz o risco de um agente de ameaça de ser capaz de explorar uma vulnerabilidade.

Contramedida pode ser um forte gerenciamento de senhas, uma espécie de guarda de segurança, de acesso, assim como mecanismos de controle dentro de um sistema operacional, a implementação de um sistema básico entrada/saída (BIOS), senhas e treinamento de conscientização de segurança.

No próximo capítulo estudaremos as ameaças.

3.4 Políticas de segurança

O que é uma política de segurança?

Em síntese, é um programa de segurança que busca garantir os três princípios que aprendemos neste capítulo:

- 1) Integridade;
- 2) Confidencialidade;
- 3) Disponibilidade.

Na política de segurança de uma empresa, a gestão estabelece como um programa de segurança será criado e as metas deste programa, atribui as responsabilidades, mostra o valor estratégico e tático da segurança e descreve como a aplicação desta política deve ser realizada.

Políticas devem abordar questões específicas de segurança que a administração vier a determinar que precisam de explicação mais detalhada e mais atenção, para termos certeza de que é uma estrutura de procedimentos bem abrangemente e construída para que todos os funcionários da empresa entendam que devem respeitá-las.

As empresas podem optar por uma política de segurança de e-mail. Nela descreverão o que a administração pode ou não fazer com mensagens de e-mail dos funcionários, como os funcionários podem ou não usar as funcionalidades de e-mail de forma diferente, assim como as questões de privacidade específicas dos endereços.

Uma política específica de sistemas deve apresentar as decisões da administração que estão mais próximas dos computadores atuais, redes, aplicativos e dados.

Este tipo de política deve fornecer uma lista de softwares aprovados que podem ser instalados em estações de trabalho individuais. Deve, ainda, descrever como as bases de dados serão protegidas (regras de autorizações de acesso aos dados), como os computadores podem ser bloqueados e como ferramentas tipo firewall, sistemas de detecção de intrusão e scanners devem ser utilizados na empresa (aprenderemos sobre estas tecnologias em mais detalhes nos próximos capítulos).

As políticas são escritas como uma visão geral e com objetivo de dar conta de muitos assuntos.

Muito mais detalhamento é necessário para desenvolver as formas e métodos que precisam acontecer para realmente apoiar e efetivar esta política.

A política de segurança prevê as bases da garantia de segurança de informação.

Os procedimentos e seus componentes, assim como as implementações e mecanismos tecnológicos, são usados para preencher um quadro de especificações desta política, criar um programa de segurança total e garantir uma infraestrutura segura.

Uma política compõe-se de quatro grandes conjuntos de elementos, quais sejam:

- » Normas.
- » Linhas básicas (baselines).
- » Diretrizes.
- » Procedimentos.

3.4.1 Normas

As normas especificam como produtos de hardware e software devem ser utilizados.

Estas normas podem ser, por exemplo, um padrão da empresa que exige que todos os funcionários tenham e usem seus crachás de identificação na empresa, com os dados sobre a sua pessoa, em todos os momentos. Ou então que indivíduos desconhecidos fora dos quadros funcionais da empresa devem ser questionados sempre sobre a sua identidade e seu propósito (por que estão ali) ou, ainda, que todas as informações confidenciais devam ser criptografadas.

3.4.2 Linhas recomendadas (baselines)

As linhas recomendadas têm como objetivo prover o nível mínimo de segurança necessário para toda a empresa.

Na maioria das vezes, as linhas de base são implementações de segurança de uma única plataforma necessárias para fornecer o nível desejado de proteção e segurança da informação.

Por exemplo, uma empresa pode exigir que todas as suas estações de trabalho tenham ao menos um nível de segurança, chamado C2.

O nível de segurança da linha de base seria C2, e a linha de base, o apoio aos procedimentos que forneçam instruções passo a passo sobre como o sistema operacional e os componentes dessa estação de trabalho têm de ser instalados para atingir esse nível de segurança específico.

Isto é o conceito de linha de base, ou baseline.

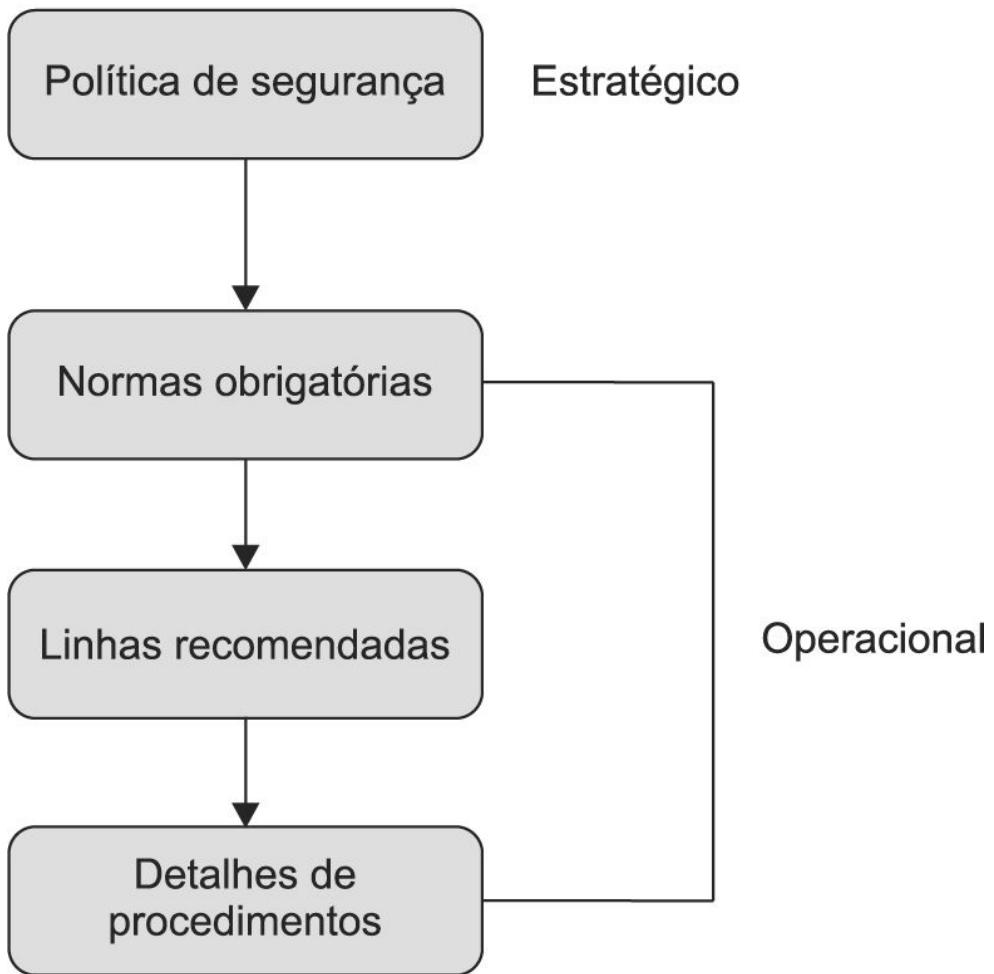


Figura 3.5 – Uma política é estabelecida nos planos estratégicos da empresa, e os elementos mais baixos, como normas, fornecem o apoio tático, ou melhor, operacional para sua aplicação.

3.4.3 Diretrizes

Diretrizes são ações de recomendação e guias operacionais para os usuários, a equipe de TI da empresa, a equipe de operações e outros usuários, quando uma norma específica não se aplica, ou não existe uma norma específica a uma determinada situação de utilização dos recursos de TI da empresa.

Elas lidam com as metodologias de segurança de computadores e de seus softwares.

Sempre existem áreas não muito claras para um usuário, onde acontecem situações que nunca haviam sido definidas, ou ações não previstas. Portanto, algumas orientações podem ser utilizadas como referência nestes momentos.

Considerando que as normas são atividades obrigatórias específicas, as diretrizes são orientações gerais que fornecem a flexibilidade necessária para as circunstâncias imprevistas.

Uma política pode determinar que o acesso a dados confidenciais deve sempre ser auditado, ou seja, deve existir registro completo deste acesso.

Uma diretriz de apoio poderia explicar melhor o que estas auditorias devem conter de informações, para serem capazes de permitir a conciliação com outros detalhes deste mesmo conjunto de diretrizes.

3.4.4 Procedimentos

Procedimentos são as ações detalhadas, passo a passo, para a realização de uma determinada tarefa.

Estes passos podem ser aplicados por usuários, pela equipe de TI, pelo pessoal operacional, pelos membros da equipe de segurança e por quem mais precise instalar ou configurar um componente de um computador.

Muitas empresas escrevem e têm procedimentos sobre a forma como os sistemas operacionais devem ser instalados, como mecanismos de segurança devem ser configurados, como configurar uma lista de controle de acessos, como criar novas contas de usuário, como atribuir privilégios, como registrar e fazer auditoria, procedimentos para destruição de materiais, relatórios de incidentes etc.

Procedimentos são o nível mais baixo da cadeia de uma política de segurança, porque eles estão mais próximos dos computadores e fornecem instruções detalhadas para problemas de configuração e instalação de software e hardware.

Normas, diretrizes e linhas básicas (baselines) não devem estar em um documento grande.

Cada uma tem uma finalidade específica e um público diferente.

Um documento que descreve como estar em conformidade com uma regulamentação específica pode ir para a equipe de gestão. Enquanto isso, um procedimento detalhado sobre como proteger adequadamente um sistema operacional específico é dirigido a um membro de TI.

Cada um dos elementos ser independente e realizado de natureza modular ajuda na sua distribuição, compreensão e atualização adequada, quando se fizer necessário.

Os documentos devem expor a forma como as políticas, normas e diretrizes serão realmente implementadas em um ambiente operacional.

A implementação de políticas de segurança e os itens que a apoiam deve receber o devido cuidado da empresa e de sua equipe de gestão.

Deve ser informado, de maneira clara, aos funcionários da empresa o que se espera deles e as consequências do não cumprimento dos elementos das políticas de segurança, destacando a responsabilidade de cada um.

Se uma empresa despede um empregado porque ele estava baixando material pornográfico no computador de trabalho, o empregado pode levar a empresa à justiça e ganhar, caso consiga provar que ele não foi devidamente informado sobre o que era

considerado de uso aceitável e inaceitável de propriedade da empresa e quais seriam as consequências. Por incrível que pareça, os elementos da política de segurança estudados, explicitando nas normas e linhas de base as restrições, devem ser obrigatoriamente divulgados para assegurar que funcionários respeitarão a política de segurança da informação da empresa.

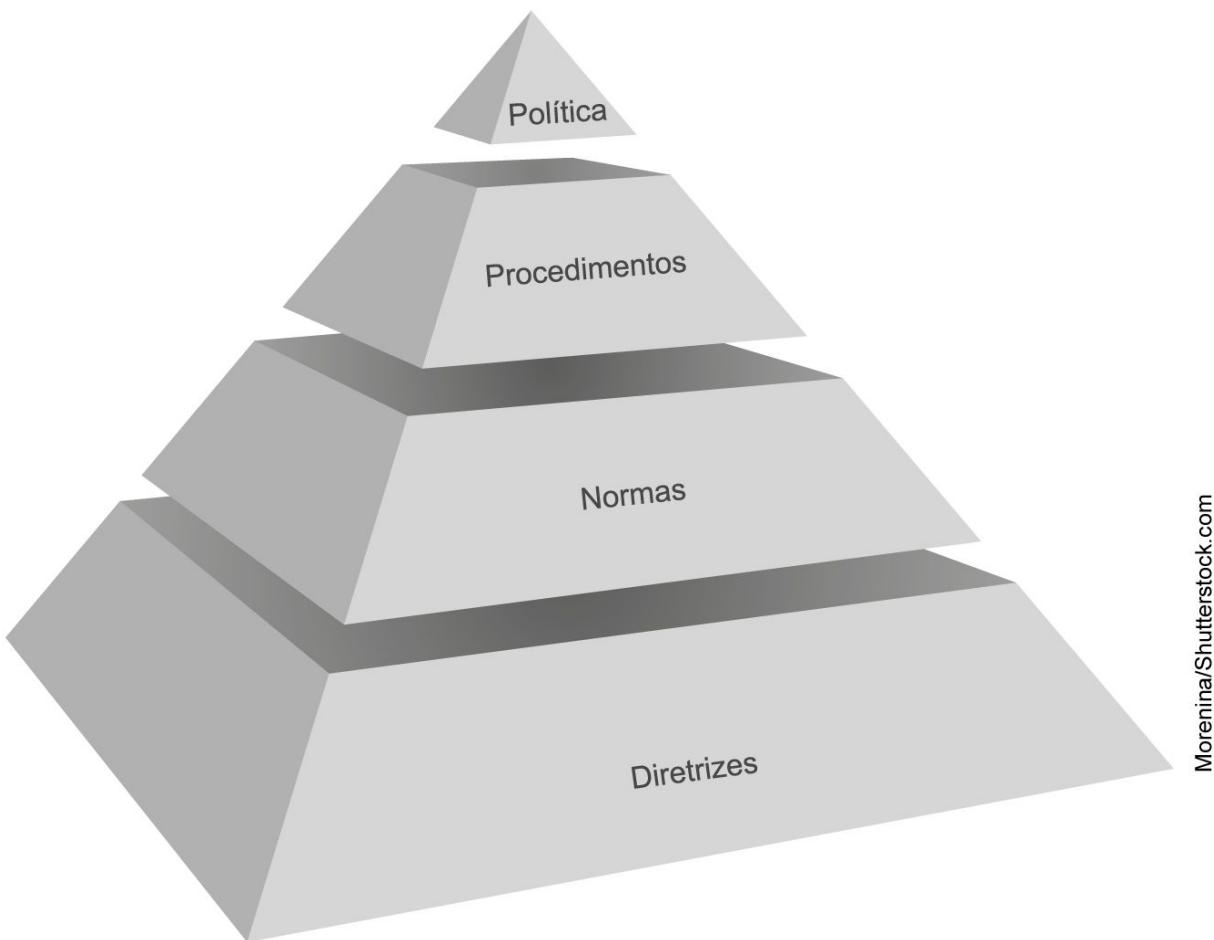


Figura 3.6 – Políticas de segurança , procedimentos, padrões e diretrizes trabalham juntos.

Vamos recapitular?

Neste capítulo estudamos mais detalhadamente os três princípios da segurança da informação. Aprendemos, também, quando estamos violando estes princípios, o que são vulnerabilidades e para que serve e o que uma política de segurança busca criar e manter os ambientes de redes seguras.



Agora é com você!

- 1) Qual é o princípio que trata de garantir que a informação não foi modificada e é confiável?
- 2) Explique qual é a relação existente entre vulnerabilidade e disponibilidade:
- 3) Normas, diretrizes e linhas básicas fazem parte de que princípio?
- 4) Veja na sua escola ou em alguma empresa como as informações são protegidas de exposição externa, e descreva como esta proteção é feita, se existir.

4

As Ameaças à Segurança da Informação

 **Para começar**

Nos capítulos anteriores falamos muito em ameaças. Vamos então estudar e conhecer o que são e quais são as principais ameaças à segurança da informação, tanto as pessoais quanto as existentes na rede de uma empresa.

4.1 Introdução

Afinal, o que são as ameaças com as quais devemos nos preocupar? Como iremos nos proteger delas?

Quem não tem um amigo que perdeu os dados de seu computador pessoal ou que presenciou o site da empresa em que trabalha ficar fora do ar ou o sistema travar? Há ainda casos de vazamento de informações de empresas, como dados de cartões de crédito de clientes que vão parar nas mãos de piratas ou outras empresas.

Estas situações oferecem a base para a existência do que chamamos e estudamos: a segurança da informação.

4.2 Ameaças

Vamos ajudar você, leitor, a entender o que é uma ameaça.

As ameaças são qualquer causa potencial de um incidente indesejado, que caso se concretize possa resultar em dano aos dados de um computador.

Ameaças exploram as falhas de segurança, que são os pontos fracos do conjunto hardware e software dos computadores, e, como consequência, provocam perdas ou danos aos valores de uma empresa, afetando seus negócios.

Ameaça pode ser uma pessoa, alguma coisa, um evento ou uma ideia capaz de causar dano a um recurso, alcançando um ou mais objetivos (ética, confiabilidade, integridade e disponibilidade).

As ameaças exploram as vulnerabilidades ou fragilidades do sistema de informações para causar impactos, da mesma forma que um assaltante explora o descuido de terceiros que andam pelas ruas, distraidamente, falando ao celular (você está vulnerável).

A *análise de ameaças e vulnerabilidades* tenta definir qual a *probabilidade* de ocorrência de cada evento adverso e as consequências da quebra da segurança da informação.

- » Vulnerabilidade: dormir de janela aberta.
- » Ameaça: assalto.
- » Aspecto afetado: integridade.
- » Impacto: perda de conforto, bens, valores financeiros.

É como antes de sair de casa, você analisar como está o movimento nas ruas, se existem pessoas suspeitas circulando, se você não está chamando a atenção com suas roupas ou mochila, por exemplo, e analisar quais as chances de ser assaltado se for caminhando até um supermercado ou casa de um amigo e ainda

mais, considerar na análise se você estiver com problemas físicos para em caso de necessidade de sair correndo e usar este recurso como opção de fugir de uma tentativa de assalto com mais segurança.

A *análise de impactos* identifica os recursos críticos do sistema, aqueles que mais sofrerão impactos na ocorrência de quebra de segurança.



Exemplo

Qual das situações seria mais impactante: roubarem seu celular, ou sua mochila, e saírem correndo, ou um assaltante dar um tiro ou uma facada em você para roubar seus pertences?

Fique de olho!

Ameaça: é evento ou atitude indesejável (roubo, incêndio, vírus etc) que potencialmente remove, desabilita, danifica ou destrói um recurso necessário e importante para você ou para uma empresa.

Vulnerabilidade: é uma fraqueza ou uma deficiência que pode ser explorada por uma ameaça. Normalmente ela está associada à possibilidade desta ameaça acontecer e aos problemas que esta ameaça irá ou poderá causar aos dados de um computador ou a uma rede de computadores.

4.2.1 Ameaças fundamentais

Ameaças fundamentais são aquelas que afetam diretamente os princípios que queremos manter para a segurança da informação. Elas são classificadas em quatro grandes tipos:

4.2.1.1 Vazamento de informações

O vazamento ou a disponibilização externa de dados de uma empresa pode acontecer de duas formas:

a) **Involuntária:** provocada por falha de hardware, desastres naturais, mensagem enviada a um endereço incorreto, erros de programação, erros de um usuário provocado por algum desconhecimento, tais como hierarquia, procedimentos, valores, entre outro, ou também por bugs (falhas) de software etc.;

b) Voluntário: este tipo, normalmente realizado por pessoas mal-intencionadas, consiste no roubo deliberado de dados, espionagem entre empresas ou organizações, fraudes por meio de adulteração de dados com identificação de usuários roubada, sabotagem, invasão de sites por hackers etc.

4.2.1.2 Violação de integridade

Comprometimento da consistência dos dados ou do sistema por intermédio de alterações não autorizadas de dados.

Podem ser considerados como violação de integridade a alteração da página de abertura de um site, um erro de software que, por exemplo, aumente por engano os salários de todos os funcionários de uma empresa ou apenas de um grupo de funcionários.

Esta violação também pode ser considerada voluntária ou involuntária.



Figura 4.1 – Ameaças fundamentais.

4.2.1.3 Indisponibilidade de serviços de informática

Trata-se do impedimento deliberado do acesso aos recursos computacionais por usuários autorizados ou não.

Os ataques DoS (sigla para Denial of Service), por exemplo, são “ataques para causar negação de serviços de um site da internet”. Eles são uma tentativa de fazer com que computadores – chamados de servidores Web – tenham muita dificuldade, ou até mesmo sejam impedidos, de executar suas tarefas.

Para isso, em vez de “invadir” o computador ou mesmo infectá-lo com malwares, o autor do ataque faz com que a máquina central de uma rede receba tantas requisições, até que não consiga atendê-las, ficando desta forma indisponível.

Outro ataque deste tipo é o ataque DDoS (Distributed Denial of Service).

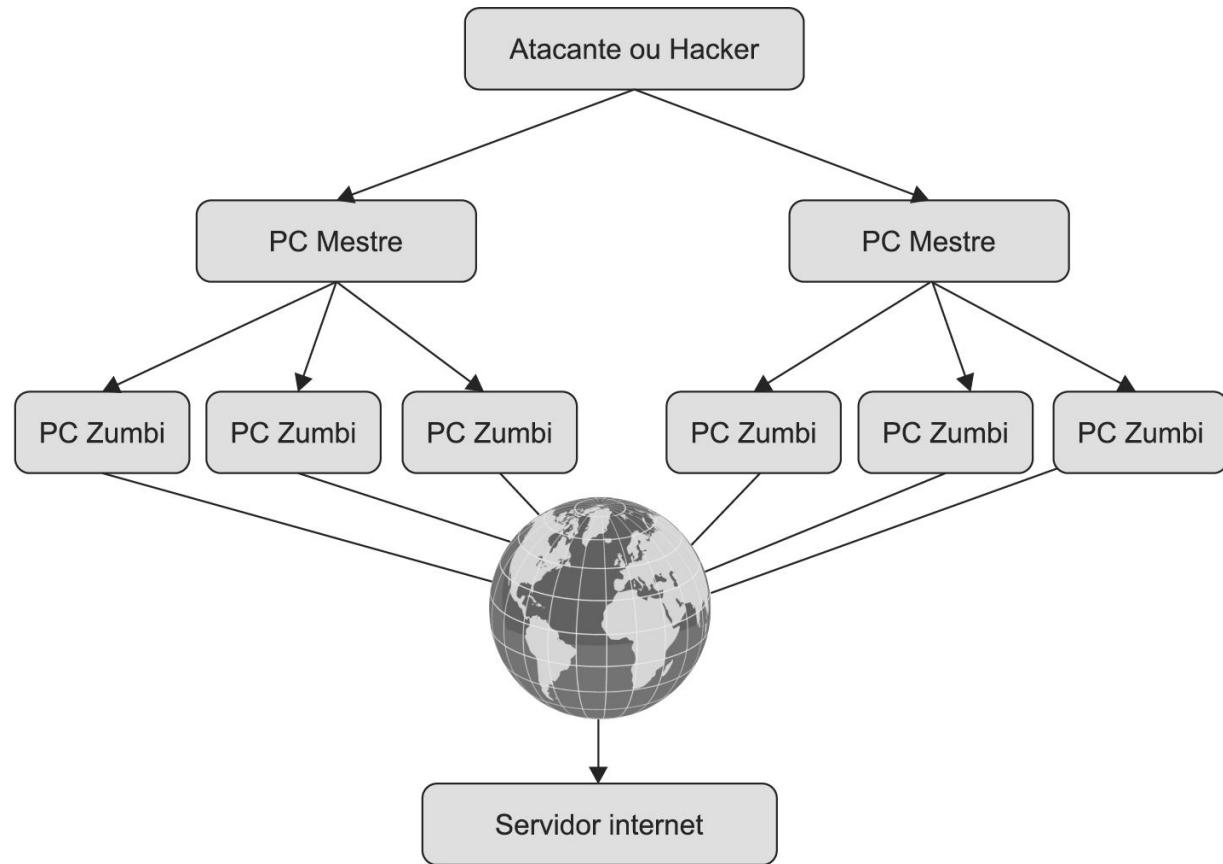


Figura 4.2 – Ataque DDoS.

Para entendermos a diferença entre eles, explicamos que este tipo de ataque se caracteriza por ser de grandes dimensões. Ele pode utilizar milhares de computadores infectados, que atuam como zumbis – por isso chama-se Distributed (Distribuído) –, para atacar uma determinada máquina (servidor Web), onde estão localizadas

as páginas de um determinado site de uma empresa. Assim serão distribuídas estas ações de acesso simultâneo entre as milhares de máquinas zumbis.

Esse tipo de ataque, que aparece constantemente em jornais ou em publicações da internet, é o ataque mais comum à disponibilidade de informações.

Em outras palavras, o computador fica tão sobrecarregado que nega os serviços ou acessos a um site. Você tenta acessar o site, mas ele não responde.

No capítulo anterior falamos sobre ataques deste tipo ocorridos recentemente. O interessante é que eles não têm como objetivo roubar dados, e sim “brincar”, se é que se pode dizer isto. Eles tiram do ar sites de grandes empresas, principalmente as que prestam serviços comerciais, ou sites governamentais, o que caracteriza um procedimento mal-intencionado, não podendo ainda ser considerado como um ato criminoso em si.

4.2.1.4 Acesso e uso não autorizado

Acontece quando um recurso de algum sistema, site ou rede (um programa, dados, um relatório) é utilizado por uma pessoa não autorizada ou de forma não autorizada.

É comum em casos de roubo de senhas pessoais de acesso, quando, então, terceiros passam a acessar informações às quais não teriam acesso autorizado. Ou, ainda, em ataques diretos aos bancos de dados de uma empresa, ou de seu computador, por meio de trojans, infectando máquinas de uma rede.

Veremos, mais à frente, o que são trojans e como eles capturam senhas de rede, sites, bancos de dados, pessoal ou corporativo, e até mesmo bancários.

4.2.2 Outros tipos de ameaças

Existem outros tipos de ameaças que, ao se efetivarem em um ataque, permitem a realização de uma ou mais *ameaças fundamentais*. Ou seja, são mistas e poderiam ter duas ou mais das classificações fundamentais.

4.2.2.1 Mascaramento

Quando alguma coisa (pessoa ou programa) se faz passar por outra.

4.2.2.2 Desvio de controles (bypass)

Quando um hacker, por exemplo, explora falhas de um sistema e suas vulnerabilidades de segurança, burlando os controles para obter direitos de acesso não autorizados.

4.2.2.3 Violação autorizada

Um usuário ou programa autorizado usa o sistema com propósitos ou em funções não autorizados.

4.2.2.4 Ameaças programadas

São códigos de software que se instalam em um sistema ou computador com o objetivo de comprometer sua segurança, alterando ou destruindo dados ou sistemas.

4.3 O que são vírus, worms (vermes) e trojans (cavalos de troia)

4.3.1 Vírus

Um vírus é um pequeno programa escrito com o objetivo de alterar a forma como um computador opera, sem a permissão ou o conhecimento do usuário.

Denominam-se vírus os programas que possuem as seguintes características:



Texelart/Shutterstock.com

Figura 4.3 – Vírus.

- » São sempre autoexecutáveis. Geralmente, um vírus adiciona o seu próprio código no caminho de execução de outro programa. Ele associa-se a outro programa normal inserindo seu código de execução no outro;
- » Um vírus normalmente duplica a si próprio. Por exemplo, pode substituir outros arquivos executáveis por uma cópia do arquivo infectado por vírus. Os vírus podem infectar tanto desktops quanto servidores de rede.

Muitos dos vírus são programados para danificar o computador, corrompendo programas, apagando arquivos ou mesmo formatando o disco rígido (a pior das possibilidades).

Outros não são desenvolvidos para causar danos. Eles são criados apenas para se multiplicar e se tornar conhecidos por meio de mensagens de texto, vídeo e áudio.

» Mesmo inofensivos, esses vírus podem criar problemas para o usuário do equipamento, pois interferem no funcionamento da memória do computador, que deveria estar sendo utilizada por programas legítimos.

Isso faz com que o desempenho dos computadores fique irregular e lento. Eles, inclusive, podem provocar um travamento completo do computador.

Além disso, diversos vírus provocam erros, que podem causar, além do travamento do sistema operacional, a perda significativa de dados.

Ambos, vírus e worms, são pragas virtuais que “infectam” o computador da vítima e causam algum tipo de dano ou prejuízo.

Mas as semelhanças param por aí.

Para entendermos melhor, faremos, no quadro a seguir, uma comparação com o ambiente biológico:

Fique de olho!

Um vírus e um verme (worm) para computadores têm mais ou menos a mesma diferença que existe entre um vírus e um verme biológico.

No ambiente biológico, um verme é um ser vivo completo, na maioria das vezes pluricelular e até visível a olho nu. Ele tem todas as funções biológicas necessárias para sobreviver. Mesmo que seja um parasita e roube alimento do corpo do hospedeiro, ainda assim é um ser vivo completo e autônomo.

Já um vírus é um ser vivo muito mais simples. Tão simples que sequer pode ser considerado como unicelular, já que ele nem é uma célula completa. Ao contrário do verme, o vírus não é autônomo. Quando uma pessoa fica infectada (com o vírus da gripe, por exemplo), o vírus usa a estrutura das células humanas para se “completar”. Ao contrário do verme, portanto, o vírus não existe sem as funções básicas providas pelas células animais.

Um vírus normalmente exige um processo, ou mecanismos de entrega (chamado de vetor), algo como um arquivo .zip ou algum outro *arquivo executável anexado a um e-mail*, para transportar o código do vírus de um local para o sistema.

- » O principal elemento que distingue um worm de um vírus de computador é essa necessidade de interação humana para facilitar e possibilitar a difusão de um vírus.
- » Vírus necessitam da interação humana, de algum processo de infecção executado inocentemente, na maioria dos casos *por e-mail*.

4.3.2 O que é um trojan (cavalo de troia)?

Os cavalos de troia, ou melhor trojans, são programas impostores ou arquivos que se passam por um programa desejável, mas que, na verdade, são prejudiciais.



maraga/Shutterstock.com

Figura 4.4 – Trojans.

Uma distinção importante entre programas *cavalo de troia* e os vírus efetivamente é que os trojans *não se autoduplicam*.

Os programas do tipo *cavalo de troia* contêm códigos maliciosos que, quando ativados, causam a perda e normalmente o roubo de dados, senhas de acesso etc.

Para que um cavalo de troia possa se espalhar, o próprio usuário deve instalá-lo no computador, mesmo que inconscientemente. Por exemplo, os casos mais comuns se dão ao abrir um anexo de e-

mail, ao fazer downloads ou executar um arquivo diretamente da internet.

Como na lenda grega *Ilíada*, o cavalo de troia parece algo simples, sem maldade. Porém, quando aberto (ou melhor, executado), apresenta os vários soldados gregos que durante a noite abriram os portões da cidade para a entrada de mais soldados e a consequente dominação da cidade de Troia, no nosso caso o seu computador ou uma rede de computadores.

Exemplos de cavalo de troia, o trojan. Vundo é um cavalo de troia .

Há diferentes tipos de trojans, classificados conforme o tipo de ações maliciosas que executam ao infectar um computador. Alguns destes tipos são:

- » *Trojan Downloader*: instala outros códigos maliciosos, obtidos em sites.
- » *Trojan Dropper*: instala outros códigos maliciosos que estão embutidos no próprio código do trojan.
- » *Trojan Backdoor*: inclui *backdoors*, possibilitando o acesso remoto do atacante ao computador.
- » *Trojan DoS*: instala ferramentas para a negação de serviço e as utiliza para desferir ataques.
- » *Trojan Destruutivo*: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
- » *Trojan Clicker*: redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.
- » *Trojan Proxy*: instala um servidor proxy, possibilitando que o computador seja utilizado para navegação totalmente anônima e para envio de spam.

- » *Trojan Spy*: instala programas *spyware* e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las para um atacante.
- » *Trojan Banker ou Bancos*: coleta dados bancários do usuário por meio da instalação de programas *spyware* que são ativados quando sites de *Internet Banking* são acessados. É similar ao *Trojan Spy*, porém com objetivos mais específicos.

Fique de olho!

Observe se seu computador apresenta algumas das características de cada um desses tipos de trojan. No caso de *Internet Banking*, verifique sempre se o cadeado está aparecendo na barra do browser.

4.3.3 O que é um worm?

Worms (vermes) são programas que se duplicam, passando de um sistema para outro, sem utilizar um arquivo host (arquivo hospedeiro).



Figura 4.5 – Worms.

Portanto, os *worms* se diferenciam dos vírus, os quais requerem a existência de um arquivo host (arquivo hospedeiro) infectado e que seja espalhado.

Embora os *worms* geralmente existam dentro de outros arquivos, como documentos do Word ou Excel, há uma diferença no modo com que *worms* e vírus utilizam o arquivo hospedeiro.

Em geral, o *worm* cria um documento que já vem com um programa macro “*worm*” integrado ao documento.

Quando o documento inteiro for passado de um computador a outro, ele pode ser considerado um *worm*.

Normalmente, *worms* são programas autossuficientes que atacam um sistema qualquer e exploram uma vulnerabilidade específica neste sistema.

Assim que houver a exploração bem-sucedida da vulnerabilidade, o *worm* copia seu programa do host de ataque para o sistema recém-explorado para começar o ciclo novamente.

Em janeiro de 2007, um *worm* infectou a conhecida comunidade MySpace.

Usuários confiáveis habilitaram a propagação do *worm*, que começou a se replicar nos sites dos usuários com a desfiguração “w0rm.EricAndrew”.

Exemplo de *worm*: O W32.Mydoom.AX@mm.

Amplie seus conhecimentos

É óbvio que um vírus precisa ser executado para infectar o sistema operacional de um computador ou rede, mas ninguém afirma que o usuário o executa com a intenção de ser infectado. Os vírus, geralmente, vêm em e-mails com arquivos anexados ou links da internet, assim como, normalmente, são arquivos .exe. Em outras palavras, executou = infectou.

Outros vêm em forma de link em uma página da Web. Nesse caso, se clicarmos nele, poderá ser levado até uma página que irá coletar informações do seu computador com a pior das intenções. Exemplos são e-mails informando sobre dívidas.

Existem muitos sites que têm a intenção de pegar “um certo ‘troux’ e infectá-lo, nem que seja só mesmo para colecionar informações do seu computador”. Desta forma, um hacker pode invadir seu computador e enchê-lo de *keyloggers*⁴ e/ou deixar vários vírus para acabar com seu sistema operacional. Tanto vírus quanto *trojans* e *worms* são ameaças que podem infectar um computador por meio de um e-mail a um desavisado ou usuário assustado que clique para abrir um anexo ou link da internet. São diferentes em seu formato, mas são os principais causadores de problemas de segurança da informação.

4.4 Tipos de vírus

Os vírus conhecidos possuem cinco classificações:

- » Vírus de infecção de arquivo;
- » Vírus de setor de inicialização;
- » Vírus do registro mestre de inicialização;
- » Vírus múltiplos;
- » Vírus de macro.

Veremos as características de cada um destes tipos.

Nosso objetivo é que você os entenda e domine a tipologia (tipo de vírus que está infectando um computador), para poder no futuro reconhecê-los pelo seu comportamento e saber como combatê-los e evitá-los.

4.4.1 Vírus de infecção de arquivo

Esses vírus têm como principal característica infectar arquivos de programas já instalados no computador, arquivos com extensão .exe, .dll, .com, entre outros.

Fique de olho!

Geralmente, infectam códigos executáveis, arquivos que possuem extensão .com e .exe. Se prestarmos atenção, observará que, quando executa uma varredura em seu programa antivírus, ele mostra a mensagem: procurando na memória.

Entretanto, também podem infectar outros arquivos não executáveis, o que acontece quando um programa infectado é executado a partir de uma mídia removível, como um pen drive, ou na própria rede.

Muitos desses vírus ficam residentes na memória do computador infectado.

Depois que a memória é infectada, qualquer arquivo executável não infectado que for executado irá tornar-se também um arquivo infectado, inclusive um programa antivírus.

Exemplos de alguns vírus de infecção de arquivos: Jerusalém e Cascade.

4.4.2 Vírus de setor de inicialização (vírus de boot)

Os vírus de setor de inicialização são aqueles que infectam a área do sistema operacional de um disco, o registro de inicialização de mídias removíveis regraváveis e discos rígidos.

O MBR (Master Boot Record – Registro Mestre de Boot) é o setor onde ficam os carregadores, isto é, os arquivos do sistema operacional do computador.



ktsdesign/Shutterstock.com

Figura 4.6 – Vírus de boot.

O registro mestre de inicialização fica no primeiro setor da unidade de disco rígido. Ele identifica onde a partição ativa está e inicia em seguida o programa de reinicialização para o setor de inicialização dessa partição. O setor de inicialização identifica onde o sistema operacional está localizado e ativa as informações de inicialização a serem carregadas no armazenamento principal ou na RAM do computador. O registro mestre de inicialização inclui uma tabela que localiza cada partição presente na unidade de disco rígido – Symantec.

Geralmente ele registra as partições primárias do disco rígido, onde há as chamadas imagens de boot (geralmente um arquivo .img ou .bin) em que existe uma cópia do sistema operacional do computador.

Ao ligar o computador, dependendo da sequência de boot, a BIOS procura por uma imagem de boot conforme a configuração de boot primária no disco rígido do computador (setup) ou na unidade de CD/DVD.

Quando ele efetua a busca no disco rígido, procura na MBR, primeiramente.

Se ela não encontrar a imagem, aparecerá uma mensagem informando que o disco está sem sistema. Em seguida, o computador parará ou solicitará que o usuário tecle “enter” para carregar o sistema do CD/DVD, ou “esc” para sair.

Se achar, o sistema é carregado e passa à execução dessa imagem de boot, que carrega o sistema operacional no computador.

Todos os discos rígidos (incluindo discos contendo somente dados) contêm um pequeno programa no seu registro de inicialização que é executado quando o computador é iniciado.

Os vírus do setor de inicialização se anexam a essa parte do disco e são automaticamente ativados quando o usuário tenta iniciar o computador a partir de um disco rígido infectado, ou de um CD/DVD também infectado.

O vírus chamado de vírus de boot só é ativado quando o computador é ligado e o sistema operacional, carregado.

Esses vírus sempre são residentes, ou melhor, estão gravados na memória do computador.

A maioria deles é escrita para DOS. Porém, todos os computadores, independente de qual seja o seu sistema operacional, são alvos potenciais desse tipo de vírus.

Para que o computador seja infectado, basta uma tentativa de inicializá-lo utilizando um disco rígido infectado, ou outro tipo de mídia removível.

A partir deste momento, enquanto o vírus permanecer na memória, todos os discos ou mídias que não forem protegidos contra a gravação se tornarão infectados ao ser acessados.

Alguns exemplos destes vírus são: Form, Disk Killer, Michelangelo e Stoned.

Fique de olho!

Muito cuidado com mídias em CD/DVD ou em pen drives que contenham arquivos ou pastas de inicialização de computadores e sistemas operacionais.

4.4.3 Vírus do registro mestre de inicialização

Os vírus do registro mestre de inicialização residem também na memória e infectam os discos da mesma forma que os vírus do setor de inicialização.

- » A diferença entre esses dois tipos é a localização do código com vírus.



JoeFotoSS/Shutterstock.com

Figura 4.7 – Vírus do registro mestre de inicialização.

Os vírus do registro mestre de inicialização geralmente salvam uma cópia legítima deste registro mestre em um local diferente.

Os computadores com sistema operacional Windows NT (Server) que são infectados por vírus do setor de inicialização ou vírus do setor de inicialização mestre não podem mais ser inicializados.

Isso ocorre em decorrência da diferença no modo em que esse sistema operacional acessa suas informações de inicialização em relação às outras versões do Windows.

Em um sistema Windows NT (Server) formatado com partições FAT, geralmente é possível remover o vírus inicializando o sistema via DOS e utilizando um software antivírus.

Se a partição de inicialização for do tipo NTFS, o sistema deverá ser reparado utilizando-se os discos de instalação do Windows (Server).

Alguns exemplos destes vírus são: NYB, AntiExe e Unashamed.

4.4.4 Vírus múltiplos

Os vírus múltiplos (também conhecidos como polypartite) infectam os registros de inicialização e os arquivos de programas.

- » Esses vírus são considerados os mais difíceis de remover.
- » Se somente a área de inicialização for limpa por um antivírus, e não os arquivos do computador, essa área será infectada novamente.
- » O mesmo ocorre se somente os arquivos infectados forem limpos.

Se o vírus não for removido da área de inicialização, quaisquer arquivos que tenham sido limpos serão novamente infectados.

Alguns exemplos destes vírus são: One Half, Emperor, Anthrax e Tequila.

4.4.5 Vírus de macro

Esse tipo de vírus também infecta arquivos de dados, principalmente arquivos do pacote Office.

Ele é um tipo extremamente comum e sua remoção tem sido a mais cara e demorada para as empresas.

Com o advento da utilização do Visual Basic desde a versão do Office 97, um vírus de macro já pode ser criado para infectar não apenas arquivos de dados, mas também outros tipos de arquivos, mesmo que não sejam do pacote Office.

Qualquer tipo de arquivo que possua macros em seu programa de leitura e gravação, como a macro de localização de textos do Word que mostraremos a seguir, pode ser infectado por este vírus.

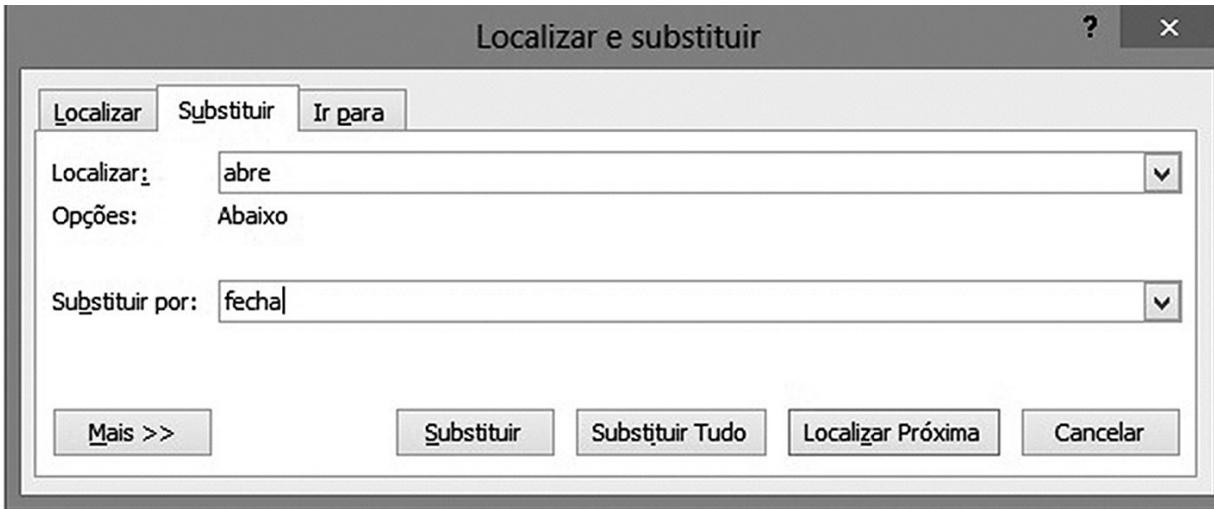


Figura 4.8 – Exemplo de uma macro.

Ao utilizarmos alguns programas, como um editor de texto, e necessitarmos executar repetidas vezes em sequência alguma tarefa (por exemplo, substituir todas as ocorrências da palavra “abre” pela palavra “fecha”), por meio da opção pesquisar e substituir, podemos utilizar um comando único para efetuá-las, uma macro interna do programa.

O Word, por exemplo, abre uma janela para a palavra pesquisada e outra para colocar a palavra a ser substituída.

Esse comando é chamado de macro e pode ser salvo em um modelo de programação para ser executado em outros arquivos.

Além dessa macro que apresentamos e que é comum no Word, um usuário com domínio da linguagem Visual Basic pode criar um modelo de macro mal-intencionado, com os comandos básicos da linguagem, nos editores de texto, e que também irão funcionar com modelos do Word.

Os vírus de macro atacam justamente esses arquivos, comprometendo o funcionamento do programa.

Os alvos principais são os próprios editores de texto (Word), as planilhas de cálculo (Excel) e, inclusive, arquivos de PowerPoint.

Novos casos de vírus de macro, que já estão infectando também outros programas, têm sido descobertos.

Todos esses vírus utilizam a linguagem de programação interna de outro programa, a qual foi criada para permitir que os usuários automatizem certas tarefas naquele programa.

Em decorrência da facilidade com que esses vírus podem ser criados, há milhares deles em circulação.

Alguns exemplos destes vírus são: W97M.Melissa, WM.NiceDay e W97M.Groov

4.4.6 Síntese sobre vírus na visão de um fabricante de antivírus

Para conhecermos os conceitos que a Symantec, uma das maiores empresas especializadas em software antivírus, nos fornece sobre vírus e para enriquecer nosso conhecimento geral:

Um vírus é um software projetado e escrito para afetar de forma adversa o seu computador ao alterar a forma como ele trabalha sem o seu conhecimento ou permissão.

Em termos mais técnicos, um vírus é um código de programa que se implanta em um dos seus arquivos executáveis e se espalha sistematicamente de um arquivo para outro.

Os vírus de computador não são gerados espontaneamente. Eles precisam ser escritos e ter um objetivo específico. Em geral, um vírus tem duas funções distintas:

Ele se dissemina de um arquivo para outro sem sua participação ou conhecimento. Tecnicamente, isso é conhecido como autorreplicação e propagação. Implementa o sintoma ou o dano planejado pelo seu criador.

As suas atividades incluem apagar um disco, corromper seus programas ou simplesmente provocar o caos no seu computador. Tecnicamente, isso é conhecido como ação do vírus, que pode ser benigna ou maligna conforme a imaginação do seu criador.

Um vírus benigno é um vírus que foi projetado para não provocar danos ao seu computador. Por exemplo, um vírus que se oculta até uma data ou hora predeterminada e, em seguida, não faz nada mais do que exibir algum tipo de mensagem é considerado benigno.

Um vírus maligno é aquele que tenta causar danos ao seu computador, embora o dano possa não ser intencional.

É significativa a quantidade de vírus desse tipo que causa danos devido a uma programação inadequada e bugs autênticos no código viral. Um vírus maligno pode alterar um ou mais dos seus programas de modo que ele não funcione como deveria.

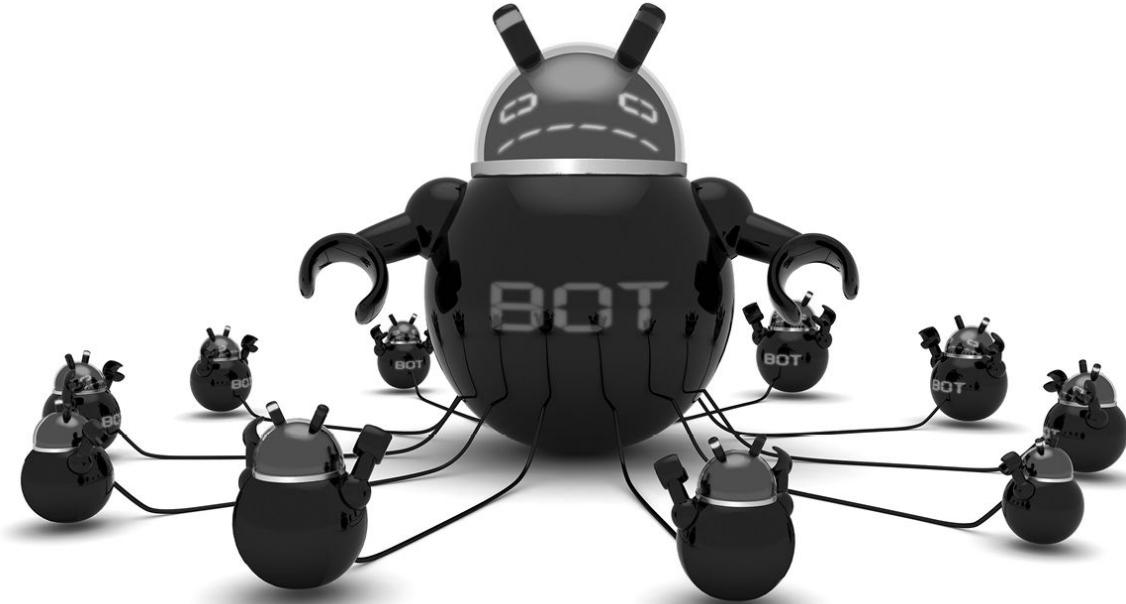
O programa infectado pode terminar de modo anormal, gravar informações incorretas nos seus documentos ou o vírus pode alterar as informações do diretório em uma das áreas do seu sistema.

Isso pode evitar que a partição seja montada ou você pode não conseguir iniciar um ou mais programas ou os programas podem não conseguir localizar os documentos que você quer abrir. Fonte: http://www.symantec.com/region/br/avcenter/virus_info.html.

4.5 Worms

Os *worms*, estes vermezinhos que vimos na definição inicial, são utilizados com frequência com técnicas de engenharia social .

O que isso quer dizer?



Gunnar Assmy/Shutterstock.com

Figura 4.9 – Worms.

Eles se utilizam de nomes atrativos, normalmente associados a pessoas famosas, software pirata, conteúdos de caráter sexual e temas da atualidade, para camuflar arquivos suspeitos. Estão sempre tentando despertar a curiosidade dos usuários, seja por intermédio de e-mails, endereços normalmente desconhecidos ou até como spam, propagandas de empresas etc.

A utilização deste tipo de técnica aumenta significativamente em épocas de datas festivas, como no dia dos namorados, natal, dia das mães e dia das bruxas.

Os *worms* têm evoluído para uma nova dinâmica de formato de ataques dos malwares.

O termo *malware* é proveniente do [inglês](#) e significa *malicious software*. Trata-se de um [software](#) destinado a se infiltrar em um sistema de [computador](#) alheio de forma ilícita, com o objetivo de causar danos, alterações ou roubar informações, confidenciais ou não.

Em um primeiro momento, os worms eram desenvolvidos principalmente para demonstrar as capacidades de programação dos seus criadores, inflando o ego de jovens programadores. Como tal eram desenvolvidos para se propagar de forma massiva e pouco discreta, infectando computadores por todo o mundo, mas sem objetivos tão maléficos.

Atualmente, os *worms* têm objetivos claramente financeiros e são utilizados para criar [botnets](#) massivas, as quais passam a controlar milhares de computadores em todo o mundo.

Para entender do que se trata uma *botnet* e como esta rede funciona, é necessário saber o que é um *bot*, seu termo de origem.

Bot, diferente de boot, é um tipo de código (programa) mal-intencionado, um vírus malicioso que transforma o computador infectado em um “*zumbi*”, um morto-vivo, a serviço de alguém que o controla remotamente, da mesma forma que nos ataques DDoS.

Computadores “*zumbis*” são computadores que podem ser controlados a distância por um invasor, independente das ações do usuário, e inclusive sem o usuário perceber.

A rede de computadores infectados por um bot é chamada de *botnet* (rede zumbi) e pode abrigar centenas ou milhares de máquinas.

As botnets geralmente são usadas para atacar sites, roubar dados, enviar spam, hospedar sites falsos. Elas são igualmente usadas para realizar ataques de negação de serviço, quando um site é acessado por milhares de máquinas simultaneamente e deixa de responder às solicitações de acesso.

A maioria dos bots se espalha utilizando falhas no Windows e por meio de redes peer-to-peer (P2P), como eMule e Ares, ou programas como mtorrent, usados para troca de arquivos entre usuários do mundo todo.

Os mal-intencionados conseguem assim transmitir ordens e comandos aos computadores infectados para enviarem spam, lançar ataques de negação de serviços e transferir arquivos maliciosos.

O funcionamento de uma botnet se dá da seguinte maneira: em primeiro lugar ele é criado por um *hacker* (denominado *bot herder*) como um código de programa que é enviado como [vírus](#) (pode ser via e-mail ou pelo acesso a sites ou links de um site), que se instalará em computadores com acesso à internet.

Uma vez instalado, o bot realiza o login em uma botnet, isto é, uma rede específica criada pelo *hacker*.

Inicia-se, então, o problema. Este *hacker* oferece a um interessado em enviar spam e pode até vender os serviços de sua rede Botnet.

Desta maneira, com a botnet espalhada pelos computadores infectados de uma rede, a mensagem de quem contratou o serviço é enviada a todos; em um processo que é controlado remotamente por um hacker.

Quanto maior for a facilidade de se propagar a *botnet*, mais destaque a comunidade que o controla possui. Existe um termo específico e público para roubos de informações online por meio de botnet, que é SCRUMPING.

Por fim, agora você já sabe que um ataque DDoS tem um *worm* no início de tudo, o processo malicioso para atacar e provocar a *indisponibilidade* de serviços de informática.

Fique de olho!

Você não fica impressionado quando recebe propagandas na sua caixa postal de e-mail, sem que nunca tenha registrado seu endereço no site que está lhe enviando mensagens?

E quando você recebe mensagens estranhas, como “olha a foto da nossa turma do tempo do colégio”, acompanhadas de um link para você clicar e ver as fotos?

Fique atento! Neste segundo caso, você pode receber sem notar um programa que transforma seu computador em um computador zumbi integrante de uma botnet.

No primeiro exemplo, você recebeu mensagens disparadas por um computador qualquer, que está como zumbi em uma botnet, e o dono nem imagina que lhe enviou.

O Conficker, o [Gaobot](#) ou [Sdbot](#) são alguns dos mais conhecidos exemplos deste tipo de worm. Os worms são hoje em dia o terceiro tipo de *malware*⁵ com maior circulação.

Os computadores comprometidos podem ser utilizados normalmente sem que seu usuário perceba a existência da infecção. Apenas em determinadas ações realizadas pelos hackers, o usuário notará alguma redução de desempenho, embora não suspeite necessariamente de uma infecção.



Exemplo

Foi identificado um grande ataque de botnets que atingiu aparelhos “inteligentes” entre 23 de dezembro e 6 de janeiro deste ano.

Dentre os aparelhos infectados estavam roteadores, centros multimídia, televisores e pelo menos uma geladeira.

Por volta de 750 mil e-mails de spam foram enviados pelos aparelhos infectados.

Fonte: <http://www.seginfo.com.br/aparelhos-inteligentes-sao-vitimas-de-botnets/>

Segundo especialistas, vários tipos de botnets infectaram milhões de computadores ao redor do mundo. Mas o conhecido como Chuck Norris é incomum e uma novidade. Ele afeta os modems *DSL* e os roteadores, em vez dos PCs, usando a senha padrão de administrador destes equipamentos.

4.5.1 Propagação de worms

O processo de propagação e infecção dos worms ocorre da seguinte maneira:

4.5.1.1 Identificação dos computadores-alvo

Após infectar um computador, o worm tenta se propagar e continuar o processo de infecção.

Para isto, necessita identificar os computadores-alvo, nos quais tentará se reproduzir, o que pode ser feito por uma ou mais das seguintes maneiras:

- » Efetuar varredura na rede e identificar quais são os computadores ativos;
- » Aguardar que outros computadores contatem com um dos computadores infectados;
- » Utilizar listas, predefinidas ou obtidas na internet, contendo a identificação dos computadores-alvo (endereços IP);
- » Utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de e-mail.

Fique de olho!

Você já deve ter ouvido falar de casos em que uma pessoa envia e-mails sem que tenha efetivamente realizado e escrito este e-mail. Simplesmente alguém informa a esta pessoa que recebeu um e-mail com vírus de um amigo, que não tem ideia de quem possa tê-lo enviado.

Estes são casos em que um worm se instalou no computador e no programa cliente de e-mail de alguém. Ao ter acesso à lista de endereços de e-mail deste computador, disparou os e-mails maliciosos e de spam.

4.5.1.2 Envio das cópias

Após identificar os alvos, o worm efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:

- » Como parte da exploração de vulnerabilidades existentes em programas instalados no computador-alvo;
- » Anexadas a e-mails. Os casos mais comuns são de e-mails sem sentido ou e-mails enviados supostamente por um amigo que o convida a ver uma foto antiga: “olhe a foto nossa que encontrei”;
- » Por meio de canais de IRC (Internet Relay Chat). Hoje são muito pouco utilizados, pelo menos no Brasil. O MSN, por exemplo, era um grande meio para estes envios.
- » Por intermédio de qualquer programa de troca de mensagens instantâneas;
- » Incluídas em pastas e arquivos compartilhados em redes locais ou redes sociais ou do tipo P2P (peer-to-peer).

Fique de olho!

Devemos ter muito cuidado com programas para baixar músicas em MP3, vídeos ou filmes, principalmente se forem de sites que tenham algum caráter sexual.

4.5.1.3 Ativação das cópias

Uma vez realizado o envio da cópia, o worm necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:

- » Imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas executados no computador-alvo no momento do recebimento da cópia;
- » Diretamente pelo usuário, com a execução de uma das cópias enviadas ao seu computador, como um arquivo obtido por download, em especial, se tiver extensão .exe.

- » Pela realização de uma ação específica do usuário, a qual o worm está condicionado, como a inserção de uma mídia removível (por exemplo, um pen drive).

4.4.7.4 Reinício do processo

O reinício do processo de propagação e ativação de worms inicia-se após o computador alvo ter sido infectado e este será reiniciado a partir deste momento, ele que em um primeiro momento representava o primeiro alvo, agora passa a ser um gerador de ataques.

4.6 O que são spywares

Spyware é um programa criado e projetado para monitorar as atividades de um sistema qualquer e enviar as informações coletadas para outras pessoas sem que a pessoa que está utilizando o computador perceba.

Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, de quais ações são realizadas, do tipo de informação que é monitorada e do uso que é feito por quem recebe as informações coletadas. Aí que mora o perigo.

Ele pode ser classificado de duas maneiras:

- » **Legítimo:** quando está instalado em um computador pessoal ou de rede, pelo próprio usuário proprietário ou com consentimento deste, com o objetivo de verificar se outras pessoas estão utilizando os recursos deste computador de modo abusivo ou não autorizado.
- » **Malicioso:** quando ele executa ações que podem comprometer a privacidade do usuário e a segurança do computador e/ou de uma rede, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário em rede, ou identificação e senha em um determinado sistema e/ou banco de dados).

4.6.1 Tipos de spywares

Alguns tipos específicos de programas spyware são:

4.6.1.1 Keylogger

Como já comentamos em nota de rodapé neste livro, é o programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

4.6.1.2 Screenlogger

Este formato é muito parecido a um keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.

É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente nos sites de *Internet Banking*.

4.6.1.3 Adware

Este tipo é projetado especificamente para encher nosso browser de propagandas quando estamos navegando na internet.

Normalmente é usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos, ou como patrocínios de sites diversos.

Também pode ser usado para fins maliciosos quando as propagandas apresentadas são direcionadas para sites específicos, abrindo outras janelas por trás de sua tela de acordo com a navegação, sem que você saiba que tal monitoramento está sendo feito, ou que o desvio está sendo realizado.

4.7 Backdoor

Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim em uma invasão anterior.

Pode ser incluído pela ação de outros códigos maliciosos, vírus que tenham previamente infectado o computador, ou por malwares, que exploram as vulnerabilidades existentes nos programas instalados no computador para poder invadi-lo.

Após incluído, o *backdoor* é usado para assegurar o acesso futuro a um computador comprometido, permitindo que ele tenha acesso remoto sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

Um backdoor típico consiste normalmente em dois componentes: clientes e servidor.

O servidor é a máquina atacada, e o cliente é o atacante. Isto é chamado de ligação direta, quando o cliente liga diretamente para o servidor.

Um atacante usará o programa do cliente para se comunicar com os componentes maliciosos do servidor, que então são instalados em algum sistema.

A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço do sistema operacional ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto.

Programas de administração remota que permitem acesso a um computador determinado de uma rede, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se forem mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como backdoors.

Há casos de backdoors incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas de operação dos mesmos. Esses casos devem ser considerados uma grave ameaça à segurança de um computador que contenha um destes programas instalados, pois além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o computador.

4.7.1 Consequências de um backdoor

Dependendo do nível de sofisticação de uma máquina cliente da rede, ele pode incluir recursos como:

- » Permitir ao atacante criar, apagar, renomear, copiar, ou modificar qualquer arquivo, executar comandos, alterar as configurações do sistema e modificar registros do Windows;
- » Permite ao atacante controlar o hardware do computador, alterando suas configurações de desligamento ou reiniciando o computador sem a permissão do usuário;
- » Permite que o atacante roube identificações de login e senhas pessoais, assim como monitore as atividades dos usuários (log);
- » Realizar backup de tudo o que o usuário digitou no teclado e capturar as telas em uso;
- » Enviar os dados coletados para um destino especificado (endereço de e-mail, servidor FTP, ou uma conexão com um host remoto);

- » Acionar a webcam para monitorar o que se passa dentro da residência de alguém. Isto, claro, parece coisa de filmes, mas é real e possível hoje.

Fique de olho!

Atualmente é muito raro que vírus ou worms sejam programados apenas para ações que assustem ou notifiquem o usuário de que algo está errado, que você pode notar por meio de comportamentos estranhos do computador, como paradas repentinas ou lentidão.

Este comportamento explica-se pelo fato de os ataques com worms, com backdoor, visarem lucro financeiro – ou seja, instalarem vírus que permitam o roubo de senhas e identificação de cartões de crédito, entre outros, ou ações políticas de impacto mundial.

Uma cartilha básica de segurança da internet recomenda que não se deve abrir anexos estranhos, que se deve atualizar sempre o antivírus e desconfiar quando um e-mail promete um prêmio especial em um concurso de que você não lembra de ter participado.

Para que você a tenha sempre à mão, a Tabela 4.1 apresenta a maioria das ameaças, como elas se propagam e os danos que geralmente produzem.

Tabela 4.1 – Códigos maliciosos e forma de entrada.

	Códigos maliciosos						
	Vírus	Worm	Bot	Trojan	Spyware	Backdoor	Rootkit
Como ele vai parar no seu computador							
Recebido automaticamente pela rede		✓	✓				
Recebido por e-mail	✓	✓	✓	✓	✓		
Baixado de sites na internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓
Como ocorre a instalação							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga							
Insere cópia de si em arquivos	✓						
Envia cópia de si automaticamente pela rede		✓	✓				
Envia cópia de si automaticamente por e-mail		✓	✓				
Não se propaga				✓	✓	✓	✓
Ações maliciosas mais comuns							
Altera e/ou remove arquivos	✓			✓			✓
Consume grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia spam e phishing			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

Fique de olho!

Reproduzo aqui um e-mail malicioso e falso, recebido enquanto escrevia este livro. Ele tem como objetivo simular uma comunicação oficial de banco, e para o qual já denunciei roubar dados bancários de clientes:

5 de fevereiro de 2014

Banco S/A

Prime

Senhor(a) FULANO DE TAL – por meio deste e-mail, informamos que o período de uso das suas chaves de segurança do Banco S/A expiraram, para continuar utilizando o mesmo cartão de chaves e serviços como Caixas Eletrônicos, Fone fácil e Internet Banking será necessário realizar o recadastramento.

Caso o recadastramento não seja efetuado, as chaves de segurança serão desativadas e seu acesso em todos os canais do Banco S/A serão bloqueados. O recadastramento é simples e rápido.

Status: Pendente.

E-mail: fulano@gmail.com

Código: 466485.855142

Para iniciar o Recadastramento clique no link logo abaixo onde está seu nome:

Iniciar Recadastramento – Cliente: fulano de tal

Agradecemos sua colaboração!

Banco S/A

Autenticação de usuário nº 466485.855142.

Vamos recapitular?

No mundo real, temos objetos reais ou palpáveis (como joias, pinturas, dinheiro, metais preciosos etc.) que são protegidos por técnicas que os colocam e isolam atrás de grades ou em caixas fortes, sob a vigilância permanente de câmeras ou equipes de seguranças.

Mas e as informações encontradas dentro de servidores de arquivos, que transitam pelas redes de comunicação ou que são lidas na tela de seu computador? Estas são denominadas ATIVOS digitais de uma empresa ou pessoa.

Como fazer para protegê-las das ameaças e seus tipos que acabamos de estudar, já que não é possível usar as mesmas técnicas de proteção de objetos reais?

Releia e procure memorizar ao máximo os tipos de ameaças. É importante que você saiba distinguir os tipos para poder decidir qual procedimento adotar e como corrigir os problemas causados por elas.



Agora é com você!

- 1) Pesquise na internet quais são os dez vírus que mais causaram prejuízos nos últimos anos, e de que tipo eram.

- 2) Os vírus que normalmente são transmitidos pelos arquivos dos aplicativos MS-Office são denominados?
- 3) A análise dos recursos críticos do sistema, aqueles que mais sofrerão impactos na ocorrência de quebra de segurança, se dá por meio de que procedimento?
- 4) Pesquise na internet ou em livros e explique o que é Phreaking.
- 5) Qual a diferença entre um vírus de boot e um programa ou vírus de bot?
- 6) Pesquise e apresente um ataque de botnet recente nos noticiários e explique.

⁴ Entre os “truques” mais utilizados pelos hackers está o keylogger, que é um programinha capaz de gravar tudo o que uma pessoa desavisada digitar no teclado, incluindo senhas de acesso a sites bancários.

⁵ Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Nesta classificação estão os vírus, worms e trojans.

5

Controle de Acessos

 **Para começar**

Agora que já apresentamos os princípios da segurança da informação e suas principais ameaças, vamos aprender o que é necessário para que sejam evitados estes ataques e como são mantidos os princípios da Segurança da Informação

5.1 Introdução

Para que os princípios da segurança da informação sejam mantidos e preservados, é necessária a criação de regras de acesso às redes, sistemas e bancos de dados armazenados em servidores de uma rede. É importante, ainda, a definição de padrões de procedimentos, por meio da utilização de ferramentas que possam bloquear ao máximo ataques externos aos computadores da rede, de políticas que estabeleçam os critérios para identificar quem internamente está utilizando os recursos de uma rede de computadores, bem como o registro de quando e o que foi executado ou realizado.

Este conjunto de regras é o que denominamos política de segurança da informação .

5.2 Controle de acessos

Como controle de acesso entende-se o gerenciamento da visualização de informações e da utilização dos recursos digitais de uma rede de computadores, considerando as propriedades da segurança da informação, quais sejam: confidencialidade, integridade e disponibilidade.

A gestão deste controle deve ser realizada para prevenir a visualização não autorizada dos dados e recursos computacionais (confidencialidade) e impedir qualquer modificação não autorizada de dados (integridade). E, paralelamente, assegurar que os dados e recursos gerenciados estarão sempre aptos para uso, quando solicitados por usuários autorizados (disponibilidade).

Quando falamos em controle de acessos, estamos nos atendo primeiramente em dois pontos: a identificação do usuário que se conecta em uma rede e sua autenticidade. Isto é, que existam formas de validar aquele nome de usuário como sendo ele mesmo.

Para que um usuário seja capaz de acessar um recurso de uma rede, deve ser determinado se essa pessoa é quem ela diz ser, se ela tem as credenciais necessárias e se foram dados a ela os direitos e privilégios necessários para executar as ações desejadas.

Em um primeiro momento, deve-se fixar um conceito: a identificação trata-se de um meio de garantir que um sujeito (usuário, programa ou processo) é realmente quem afirma ser.

Uma identificação pode ser verificada com o uso de uma credencial (com nome de usuário e número de identificação pessoal), um cartão inteligente (também conhecido, em inglês, como

smart card), assinatura digital, número de uma conta ou um atributo anatômico (impressão digital, impressão palmar etc).

Para ser devidamente autenticado, o usuário é, normalmente, obrigado a fornecer uma segunda peça para fechar o seu conjunto de credenciais de acesso.

Esta segunda peça pode ser uma senha, uma frase-senha, uma chave de criptografia ou a informação gerada no momento em um token.



Nadasazh/Shutterstock.com

Figura 5.1 – Um Token.

Estas duas peças de identificação de credenciais são comparadas com as informações previamente armazenadas no sistema pelo usuário. Se essas credenciais coincidirem com as armazenadas, o usuário é autenticado na rede. Mas o processo ainda não está concluído.

Uma vez que o usuário fornece suas credenciais e está devidamente identificado, o sistema que ele está tentando acessar (rede, sistemas, programas etc.) precisa determinar se para este assunto lhe foi dado o direito e os privilégios necessários para realizar as ações solicitadas.

O sistema de gerenciamento da rede (sistema operacional) recorrerá a algum tipo de matriz de controle de acesso, ou fará comparações nos registros de segurança, para verificar se este usuário está realmente apto a acessar o recurso solicitado e a executar as ações desejadas.

Se o usuário estiver registrado e seu acesso liberado nesta matriz, ele será autorizado a executar as ações desejadas e a utilizar os recursos solicitados.

Apesar de identificação, autenticação e autorização possuírem definições próximas e complementares, cada uma tem funções distintas que cumprem uma exigência específica no processo de controle de acesso.

Entretanto, um usuário pode ser devidamente identificado e autenticado para a rede, mas não pode ter a autorização para acessar arquivos no servidor de arquivos da rede.

Por outro lado, um usuário pode ser autorizado a acessar os arquivos no servidor de arquivos. Mas, até que ele esteja devidamente identificado e autenticado, esses recursos estão fora de alcance.

É necessário que o usuário seja responsabilizado pelas ações tomadas dentro de um sistema.

A única maneira de garantir o registro de contas é se o usuário possuir unicamente uma identificação e suas ações no sistema ou na rede forem registradas.

A Figura 5.2 apresenta os três passos para que um usuário possa utilizar recursos de uma rede, no caso uma impressora da rede, e das aplicações desejadas:

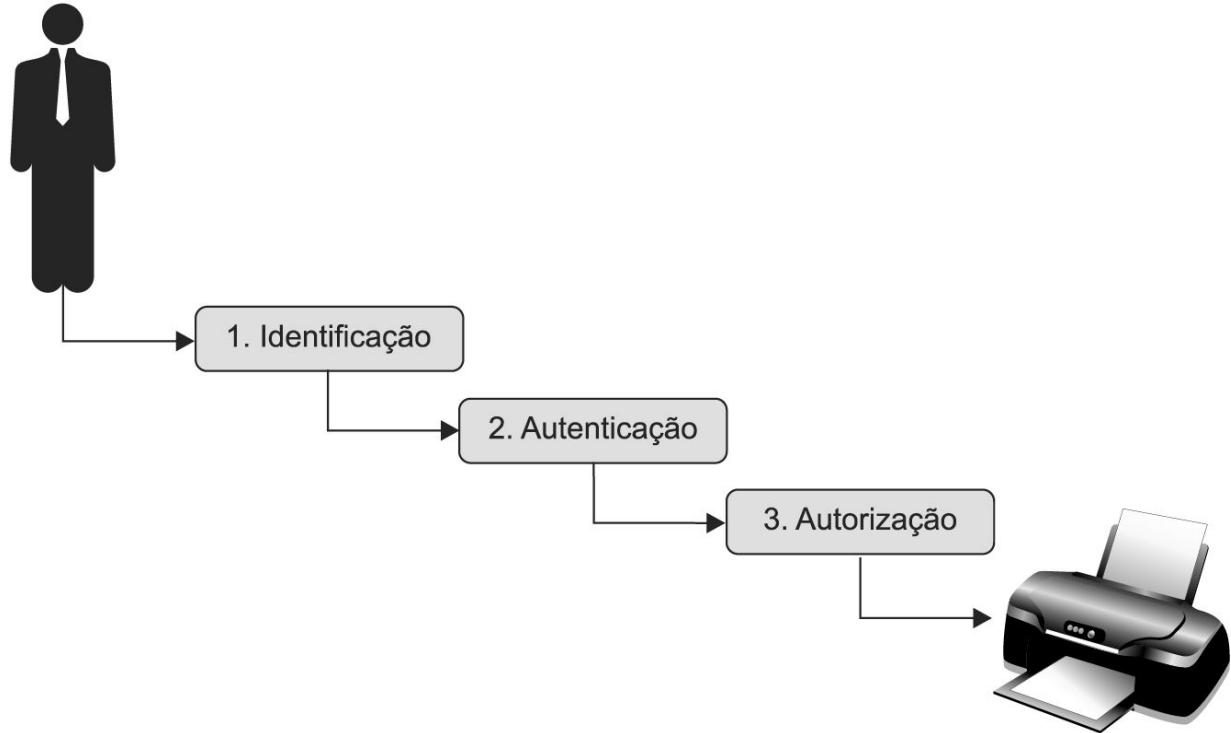


Figura 5.2 – Três passos para acessar um objeto.

Portanto, os três passos para um usuário acessar ou utilizar um recurso da rede são: identificação, autenticação e autorização.

Os chamados controles de acesso lógico são ferramentas de software utilizadas para identificação, autenticação, autorização e registro de atividades de usuários.

Eles são normalmente softwares componentes que realizam medidas de controle de acesso para sistemas, programas, processos e informações.

Os controles de acesso lógico podem ser incorporados nos sistemas operacionais, aplicativos, em add-ons de pacotes de programas de segurança, ou em sistemas de gerenciamento de banco de dados e gerenciamento de telecomunicações.

5.2.1 Identificação

Falaremos agora sobre o primeiro passo de um controle de acesso: a identificação do usuário.

A identidade de um indivíduo deve ser verificada durante o processo de autenticação.

A autenticação geralmente contém um processo de duas etapas: primeiro a inserção de informações consideradas públicas (um nome de usuário, número de funcionário, ou número de conta, identificação de um departamento, ou uma característica biométrica) e depois a inserção de algum tipo de informação privada (uma senha estática, um número de um token inteligente, uma password cognitiva, *one-time password* etc.).

A entrada de uma informação pública é a etapa de identificação e inserção de informação privada. Trata-se da fase de autenticação deste processo de duas etapas.

Normalmente as empresas criam nomes de usuários de rede baseados no nome próprio do funcionário, porém criando regras de formação deste formato de nome.

É comum utilizar-se na formação de nomes de usuário o modelo da Tabela 5.1, considerando-se que temos de adotar critérios para solucionar nomes similares ou até os casos de pessoas homônimas.

Tabela 5.1 – Funcionários e nome de usuários

Nome do funcionário	Username
Alexandre Silva	Asilva
Carlos Santos	Csantos
Carlos Silva Santos	Csilva
Carlos Silva	Silvac
Claudia Ferreira	Claudia

Claudia Souza Ferreira	Csouza
Claudia Souza	Souzac

Algumas empresas, dependendo da configuração dos servidores de rede, utilizam composições com nome, um ponto e sobrenome, mas isto é mais comum na criação de contas de e-mail corporativo.

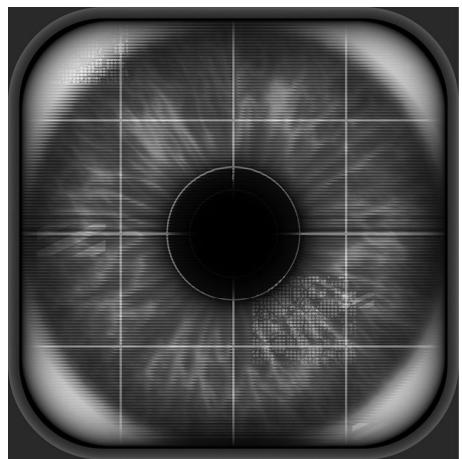
Como comentamos, podemos também utilizar a matrícula, ou número do funcionário, como identificador público. A opção de utilizar identificadores genéricos como identificação de um departamento é passível de ser utilizada, porém não recomendada. Nesse caso, seria como ter uma identificação para mais de um usuário, ou seja, todos os funcionários do departamento usariam a mesma identificação.



Andrey Burmakin/Shutterstock.com



PiXXart/Shutterstock.com



Juergen Faehle/Shutterstock.com



Franck Boston/shutterstock.com

Figura 5.3 – Tipos de tecnologias de identificação biométricas.

Vejamos alguns conceitos de identificação biométrica.

A identificação biométrica verifica uma identificação individual por meio de um único atributo pessoal. Ela é considerada um dos mais acurados e efetivos métodos de verificação de identificação.

É claro que estamos falando de tecnologia sofisticada e cara. Você já deve ter assistido a filmes em que as pessoas são identificadas para acessar um computador por meio de impressão digital, da palma da mão, ou da leitura da retina (quando alguém coloca o olho em frente a uma tela e um raio escaneia o olho).

Uma vez que este sistema verifica as ranhuras de impressão digital, o padrão de retina ou as características de voz de uma pessoa, uma das suas principais características é a extrema sensibilidade. Um sistema deste tipo deve executar medições precisas e repetíveis de características anatômicas ou fisiológicas de um indivíduo. Entretanto, este tipo de sensibilidade pode facilmente provocar falsos positivos ou falsos negativos.

Este sistema de identificação deve ser calibrado para que esses falsos positivos e falsos negativos tenham ocorrências muito baixas e que os resultados sejam sempre o mais preciso possível.

Novamente, recorrendo aos filmes como exemplo, você acreditou que alguém possa cortar o dedo indicador ou a mão de outra pessoa e usá-lo para uma identificação por impressão digital?

A princípio se estivermos lidando com um sistema de identificação biométrico, por meio de impressão digital ou de impressão palmar (mão inteira), isso seria possível com certeza. Mas não recomendamos que você faça isso.

Sistemas de identificação por impressão digital armazenam a impressão digital completa, um volume muito grande de informações que ocupam muito espaço no disco rígido e que tornam o processo para a realização de comparações de dados mais lento quando um usuário está tentando ser autenticado.

A tecnologia de scanner de dedo, por assim dizer, extrai algumas características específicas da impressão digital e armazena apenas esta informação associada a um usuário, funcionário da empresa. Com isso ocupa menos espaço em discos rígidos e permite pesquisas mais rápidas em banco de dados e as comparações necessárias no processo de autenticação do usuário.

Na verificação baseada em retina ou íris temos o seguinte formato de operação:

5.2.1.1 Scanner de retina

Um sistema que lê a retina da pessoa verifica o padrão dos vasos sanguíneos da retina, que fica na parte de trás do globo ocular.

O padrão tem-se mostrado extremamente único entre as pessoas. Ou seja, não existem duas pessoas com o mesmo padrão de vasos sanguíneos da retina.

Uma câmera é usada para projetar um feixe de luz dentro do olho e capturar o padrão de vasos sanguíneos da retina e compará-lo a um arquivo de referência registrado anteriormente, no cadastramento do funcionário, por exemplo.

5.2.1.2 Scanner de íris

A íris é a parte colorida do olho que envolve a pupila. Ela tem um padrão único, com fendas, cores, anel, coroas e sulcos.

A singularidade de cada uma dessas características dentro da íris é capturada por uma câmera e comparada com as informações obtidas durante a fase de cadastramento do funcionário.

Ao se utilizar um sistema biométrico padrão da íris, o leitor ótico deve ser posicionado de modo que o sol incida sobre a lente. Por isso, quando implementado, deve ser devidamente colocado em um

edifício com uma análise da incidência solar no local antecipadamente. A incidência solar sobre a lente irá perturbar o funcionamento correto do sistema de identificação.

Para além das tecnologias estudadas anteriormente, existem outras que não iremos detalhar, quais sejam:

- » Geometria da mão
- » Impressão de voz
- » Escaneamento facial
- » Topologia da mão

Amplie seus conhecimentos

Deixo aqui o desafio para ampliação dos seus conhecimentos por meio de pesquisa de campo. Faça um resumo descritivo de cada uma destas quatro outras tecnologias de identificação apresentadas.

5.2.2 Autenticação

Uma vez que uma pessoa foi identificada, ela deve ser autenticada. Deve-se confirmar que ela é realmente quem se diz ser.

Existem três tipos gerais de autenticação para uma pessoa: algo que ela saiba, algo que ela possua, algo que ela seja.

Algo que uma pessoa possa saber pode ser uma password (senha), um número PIN (como em alguns telefones celulares), o nome da mãe ou uma combinação de um segredo tipo de cofre.

A desvantagem deste método é que uma terceira pessoa pode obter o conhecimento desta senha e ter acesso não autorizado a um sistema.

Este é um dos motivos pelo qual as pessoas têm cada dia mais interesse em utilizar identificação e autenticação biométrica, que tem se mostrado um meio mais seguro. Lembre que senhas podem

ser perdidas, observadas e copiadas e podem causar danos irreparáveis aos sistemas de informação.

Fique de olho!

Identificação e senha são pessoais e intransferíveis. São confidenciais e nunca se deve emprestar ou dar sua senha para um colega de trabalho, amigo, ou quem quer que seja, independentemente do motivo.

5.2.2.1 Passwords

A autenticação acoplada com uma password (senha) é o mecanismo mais comum de autenticação utilizado.

Password é uma sequência de caracteres protegida utilizada para autenticar um indivíduo, um usuário.

Uma password, esta sequência de caracteres, é baseada unicamente em um conceito ou alguma coisa que o usuário sabe e somente ele sabe.

Muitos usuários não dão importância à segurança até o momento em que um craker invade seu computador.

Já foi muito comum, e ainda é um pouco, em alguns lugares encontrarmos um papel colado no monitor do computador com a password de seu usuário. Ou então encontrarmos password como data de aniversário, nome da mãe, nome do cachorro, da esposa etc.

Usuários não têm muito cuidado na escolha de senhas. É, por exemplo, o que Ashley Feinberg nos mostra em uma compilação feita pelo SplashData (uma lista que puxa dados de milhões de senhas roubadas que se tornaram públicas ao longo do ano).

Apresentamos, a seguir, as vinte senhas mais comuns na rede e que deixam muito a desejar em relação à segurança.

As “vinte mais” imprudentes são:

Tabela 5.2 – As vinte senhas mais usadas

Senhas mais comuns	
1	123456
2	password
3	12345678
4	qwerty
5	abc123
6	123456789
7	111111
8	1234567
9	iloveyou
10	adobe123
11	123123
12	Admin
13	1234567890
14	letmein
15	photoshop
16	1234
17	monkey
18	shadow
19	Sunshine
20	12345

Fonte: <http://gizmodo.uol.com.br/as-25-senhas-mais-comuns-de-2013>

Se as senhas forem corretamente geradas/criadas, atualizadas e mantidas em segredo, elas podem fornecer uma segurança eficaz.

Fique de olho!

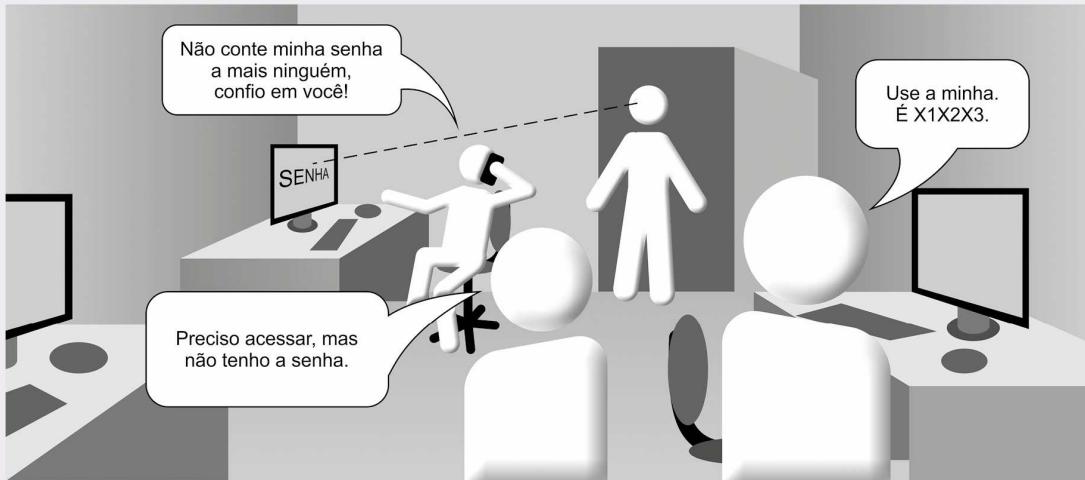


Figura 5.4 – Ambiente sem segurança de senhas.

Tudo o que for executado com a sua senha será de sua inteira responsabilidade. Portanto, tome todas as precauções possíveis para manter sua senha secreta.

Geradores de senha podem ser usados para criar as senhas de usuário.

Isso garante que o usuário não usará “*Maria*” ou “*Teste*” para uma senha. Por outro lado, se o gerador criar uma senha como “*kdjasijew284802h*”, o usuário certamente irá anotá-la em um pedaço de papel e colocá-lo colado em seu monitor.

Se um gerador de password for utilizado, as ferramentas que o compõem devem criar “*Não palavras*” pronunciáveis para ajudar o usuário a se lembrar dela. Elas não devem ser tão complexas a ponto de o usuário precisar anotá-las. De nada adiantam senhas difíceis de ser memorizadas pelo usuário.

Caso os usuários possam escolher suas próprias senhas, o sistema operacional deve exigir certos requisitos de senha para garantir maior grau de segurança. Por exemplo, pode exigir que uma senha contenha um determinado número de caracteres, letras

maiúsculas, minúsculas e números. Assim, não estará estabelecendo uma senha fraca tampouco de difícil memorização, por parte do usuário.

Normalmente, o sistema operacional, ao verificar as senhas de cada usuário, impede e garante que nenhuma senha seja reutilizada.

Os usuários também devem ser forçados a mudar suas senhas periodicamente. Esta é uma prática comum em empresas, apesar de incômoda para o usuário que tem de usar de criatividade para criar senhas a cada três meses, por exemplo. *Isso chama-se envelhecimento de senha.*

O sistema mantém normalmente uma lista com as cinco últimas senhas, ou mais, e não permite que o usuário repita uma senha utilizada anteriormente.

Todos estes fatores tornam mais difícil para um atacante adivinhar ou obter senhas dentro de um ambiente de rede.

Como outro fator de segurança temos o que denominamos limite de tentativas de login na rede. Um limite pode ser configurado para que apenas um determinado número de tentativas de login sem sucesso possa ser realizado. Após, sem sucesso, atingir este limite de tentativas, a senha do usuário é bloqueada imediatamente.

5.2.2.2 Dispositivo de token

Um dispositivo de token, ou gerador de senhas, geralmente é um dispositivo portátil que tem um display de LCD e teclado.



Dave Clark Digital Photo/Shutterstock.com

Figura 5.5 – Dispositivo de token.

Este dispositivo é uma peça de hardware separada do computador do usuário que tenta acessar a rede ou uma aplicação.

O dispositivo de token (sinal) e o serviço de autenticação têm de ser sincronizados, ou seja, utilizar o mesmo esquema de questão-resposta para ser capaz de autenticar um usuário.

O dispositivo de token apresenta ao usuário uma lista de caracteres para ser inserido, como uma senha ao fazer login em um computador.

Somente o dispositivo de “token” e o serviço de autenticação (uma aplicação desenvolvida para este fim) conhecem o significado dos caracteres apresentados no aparelhinho.

5.2.3 Outros métodos de autenticação

Existem outros métodos de autenticação que serão elencados a seguir. Como este livro não tem como objetivo detalhar o funcionamento destes métodos, sugerimos que você, leitor, pesquise sobre eles. Assim, ampliará seus conhecimentos.

5.2.3.1 Chaves criptografadas

É realizada por meio de uma chave privada, ou uma assinatura digital. O ato de criptografar este valor de “hash” com uma chave privada é chamado assinatura digital de uma mensagem. Uma assinatura digital usa uma chave privada para criptografar um valor de “hash”.

Hash (resumo), uma função do sistema operacional, é qualquer algoritmo que mapeie dados grandes e também de tamanho variável para pequenos dados de tamanho fixo.

Por esse motivo, as funções hash são conhecidas por resumirem o dado. A principal aplicação dessas funções é a comparação de dados grandes ou secretos. Assim, os dados do usuário, como nome, matrícula de funcionário, departamento e empresa, podem ser criptografados em uma função “hash”, criando, então, sua assinatura digital.

5.2.3.2 Password de frase (passphrase)

É também uma sequência de caracteres, porém mais longa que um password (senha).

Em seu primeiro acesso ao sistema, o usuário entra com uma frase, que o sistema transformará em uma senha virtual.

Por exemplo, o usuário entra com a frase “Gosto de minha privacidade”, e o sistema a converterá em uma senha virtual.

Como é sempre mais longa que um password comum, teoricamente ela é mais difícil de ser copiada por um atacante.

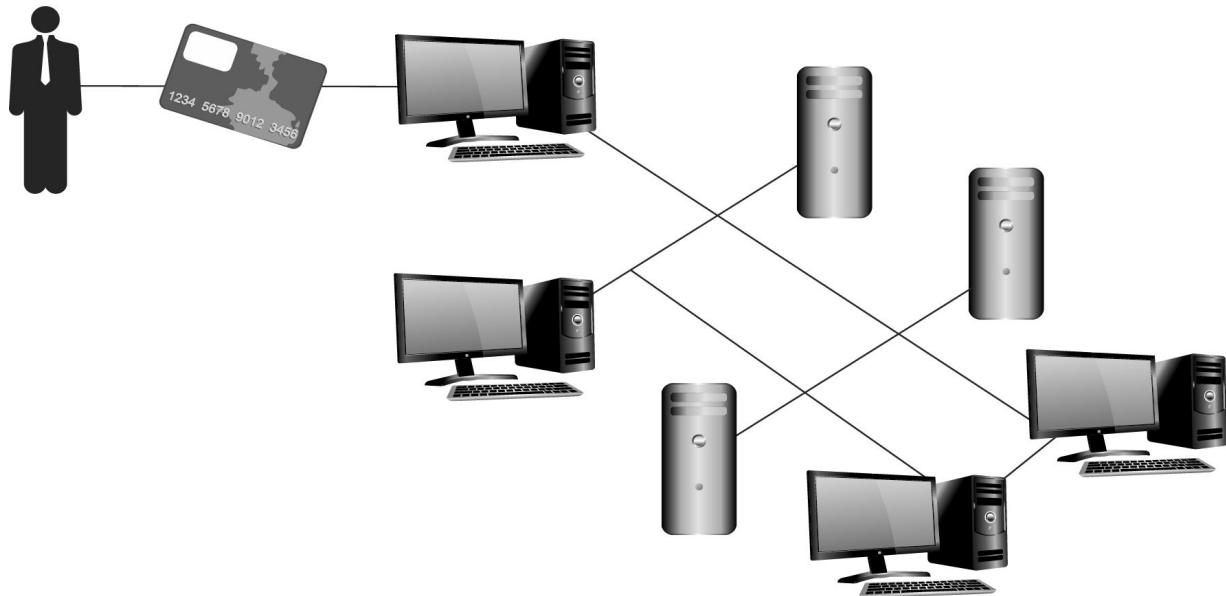


Figura 5.6 – Autenticação com utilização de cartão inteligente.

5.2.3.3 Cartões de memória

A principal diferença entre os cartões de memória e cartões inteligentes é a capacidade de processamento.

Um cartão de memória contém informações de autenticação de um usuário, de modo que este usuário só precisa digitar uma identificação de usuário (ID) ou um número de identificação pessoal (PIN), presente no cartão de memória. Se os dois combinarem, será aprovado pelo serviço de autenticação e o usuário será autenticado com êxito.

5.2.3.4 Cartões inteligentes (smart cards)

Um cartão inteligente tem a capacidade de processamento de informações porque possui um microprocessador e circuitos integrados incorporados no próprio cartão.

Um cartão inteligente fornece um método de autenticação de dois fatores; o usuário tem de digitar uma identificação de usuário ou senha para desbloquear o cartão do leitor.

Isto significa que o usuário deve fornecer algo que ele sabe, como o seu número de identificação pessoal (PIN), e algo que ele tem (smart card).

Isso é o que acontece quando você vai a um caixa eletrônico, fornece o cartão do banco e uma identificação e ele solicita uma senha para desbloquear e liberar o cartão.

Claro que, após realizar suas operações, você terá fornecido o cartão e uma identificação (no caso uma senha e mais um número de um token) para poder utilizar os recursos disponíveis.

5.3 Monitoramento de controle de acesso

Monitoramento de controle de acesso é um método de manter o controle de quem tenta acessar recursos de rede específicos. Trata-se de um importante mecanismo de detecção. Vale destacar que existem diferentes tecnologias que podem realizar esta atividade.

Vamos estudar sobre estas ferramentas e os Firewalls no próximo capítulo.

Vamos recapitular?

Neste capítulo aprendemos os conceitos de identificação, autenticação e autorização, assim como os principais métodos aplicados para identificação e autenticação que possibilitam a realização conjunta de identificação e autenticação, conhecidos como métodos biométricos. Além disso, aprendemos sobre a utilização de cartões inteligentes (smart cards), dispositivos de token e como é realizada a interação de controle entre uma pessoa e um computador ou rede de computadores.



Agora é com você!

- 1) O que é derivado de um password (senha) de frase?
- 2) Cite dois tipos de autenticação de controle biométrico?
- 3) O que uma pessoa sabe é o que proporciona uma melhor autenticação? Explique.
- 4) O que significa a autenticação?
- 5) Uma senha é usada principalmente para qual função?
- 6) Um cartão de crédito ou de débito é um smart card?

6

Firewalls e Detecção de Intrusão

 Para começar

Agora estudaremos as ferramentas e tecnologias existentes para enfrentar as ameaças apresentadas nos capítulos anteriores e como garantir os princípios da segurança da informação.

6.1 Introdução

Muitas empresas ao prezarem pela segurança de seus dados decidiram que o uso da internet é restrito àquilo que for necessário para o desempenho do trabalho. É vedado o acesso a redes sociais, sites de entretenimento, jogos ou qualquer outro tipo de passatempo.

Com isso, elas buscam garantir a segurança dos dados corporativos e direcionam o foco dos funcionários para as atividades fins da empresa.

Poderíamos dizer que tal decisão é um exagero em um mundo onde estar conectado é vital para o bem-estar das pessoas. No entanto, como tudo pode ser realizado com equilíbrio, devemos balancear as necessidades da empresa e sua produtividade no ambiente de trabalho com a sua conexão com o mundo exterior.

Analizando do ponto de vista da empresa e da segurança da informação, é claro que encontraremos diversas razões para a existência destes bloqueios no acesso à internet a fim de se estabelecer uma política de segurança e produtividade. Vamos estudar as formas desta utilização e quais os instrumentos de controle para uma maior segurança

6.2 A utilização de acesso à internet em redes corporativas

Atualmente estão disponíveis na internet os mais diversos tipos de conteúdos: notícias em tempo real, sistemas fundamentais para os negócios da empresa, documentos, facilidades financeiras, assim como jogos, salas de bate-papo, redes sociais, vídeos e músicas.

Se analisarmos o acesso ao YouTube[©], em razão de seu grande consumo de banda é um fator de preocupação compreensível, já que a rede da empresa deve sempre ter velocidade suficiente para que os funcionários executem suas funções. O acesso intensivo a sites deste tipo, portanto, compromete o desempenho da rede corporativa.

No entanto, a maior preocupação destes acessos está no risco que existe por trás dos links que direcionam para sites ou programas maliciosos, capazes de comprometer o computador e/ou o sistema de uma empresa.

As redes sociais, uma das principais responsáveis por desviarem o foco dos funcionários, também levam a links suspeitos.

Existe um risco potencial para que ocorra a instalação de aplicativos maliciosos, como malware, spyware e vírus, caso o usuário se conecte, sem nenhum controle, a redes sociais.

As empresas se preocupam cada vez mais com a segurança de seus dados e querem que os seus funcionários trabalhem em um ambiente privado e produtivo, e na intenção de evitar problemas, acabam por limitar o acesso a redes como Facebook[©] e Twitter[©], por exemplo.

Se, dentro da empresa, o uso da internet se limita às máquinas corporativas, claro que é possível permitir que os funcionários acessem seus perfis no LinkedIn[©], Facebook[©] e Twitter[©], ao mesmo tempo que possam usar o Google para fazer pesquisas em diversos sites ou obter ajuda de um vídeo no YouTube (ou até assistir a um videoclipe para momentos de descontração).

Para que isso ocorra, mesmo que importe em custos adicionais, bastará a empresa proteger os seus computadores e as suas redes contra ataques maliciosos e orientar os funcionários quanto ao uso da internet: *afinal, quando se está trabalhando, é preciso ter bom senso e evitar dispersão* .

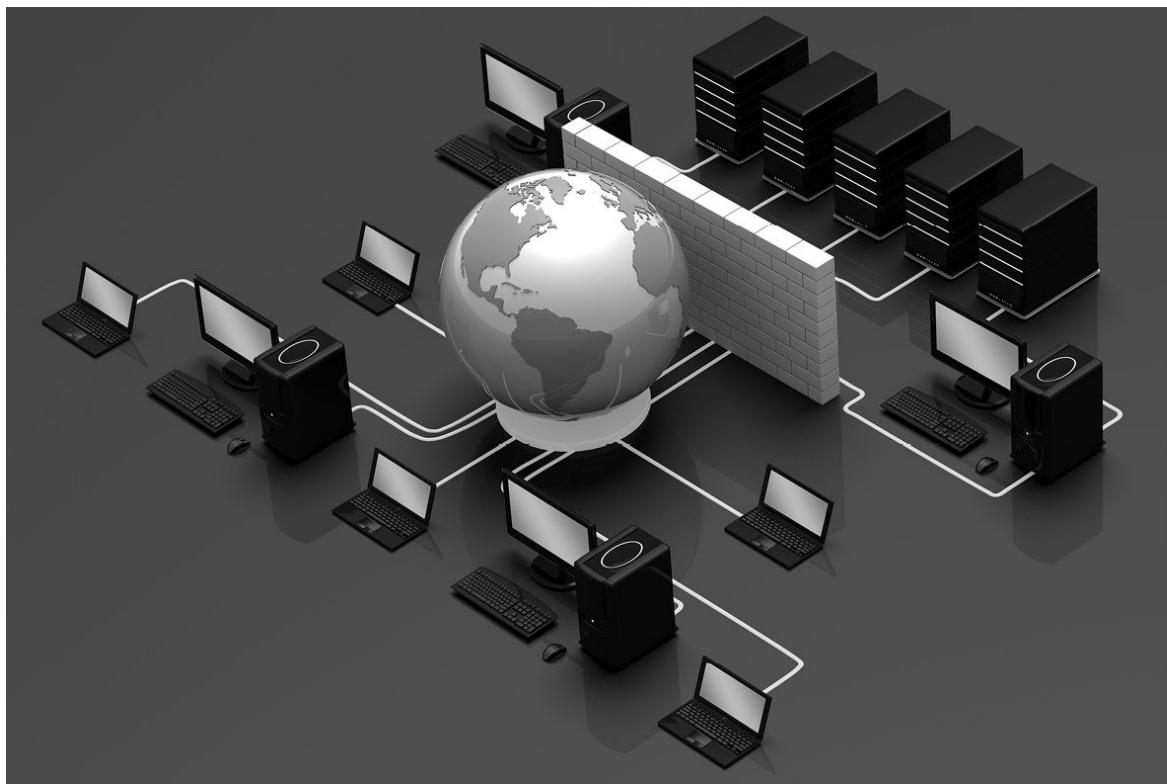
Para contornar estas questões de acesso indiscriminado à internet nos computadores corporativos, muitas, se não a maior parte das empresas, utilizam ferramentas como firewalls.

6.3 O que é um firewall?

Firewall é um mecanismo de segurança realizado em *hardware* ou *software* (que é o mais utilizado) que possui/implementa um conjunto de regras ou instruções, faz a análise do tráfego de rede (tudo o que passa na rede em que estamos conectados) e determina de acordo com as regras implementadas quais são as operações de transmissão ou recepção de dados que podem ser executadas.

“Parede de fogo”, a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa.

O objetivo de um firewall é bloquear qualquer tráfego de dados indesejado e não autorizado e liberar somente os acessos autorizados.



Tonis Pan/Shutterstock.com

Figura 6.1 – Representação básica de um firewall.

Um dos melhores exemplos que encontrei sobre o que seria equivalente a um firewall na vida real está a seguir. Sem dúvida permitirá entender claramente a finalidade de um firewall:

“... você pode imaginar um firewall como sendo uma portaria de um condomínio: para entrar, é necessário obedecer a determinadas condições, como se identificar, ser esperado por um morador e não portar qualquer objeto que possa trazer riscos à segurança; para sair, não se pode levar nada que pertença aos condôminos sem a devida autorização.”

ALECRIM, [Emerson. O que é firewall? – Conceito, tipos e arquiteturas.](#) Publicado em 19_02_2013. Disponível em: em <<http://www.infowester.com/firewall.php>>. Acesso em: 10 mar. 2014.

Devemos entender que um firewall é utilizado para restringir os acessos em uma rede por outra rede, ou seja, por usuários de outra rede. O firewall não tem atuação interna nos acessos dentro da própria rede. Estes controles são relativos aos controles de acesso, identificação e validação de usuários da própria rede.

Entretanto, podemos aplicar um firewall para restringir acesso a um segmento de uma rede interna pelos usuários desta rede corporativa.

Um firewall é uma ferramenta que suporta e reforça uma política de segurança de rede, que fornecerá instruções de alto nível sobre as ações aceitáveis e não aceitáveis no que se refere à segurança.

Um firewall é utilizado para impedir a execução de ações maliciosas oriundas de outra rede: um [malware](#) que utiliza determinada entrada lógica (porta) para se instalar em um computador sem o usuário saber e nem perceber, ou um programa que envia dados sigilosos da empresa para a internet. Ou,

finalmente, o mais comum, uma tentativa de acesso à rede de uma empresa, ou sua rede doméstica, a partir de computadores externos não autorizados.

6.3.1 Como um firewall funciona?

Já estudamos que um firewall atua como uma barreira que verifica quais dados podem passar ou não, e que esta tarefa só pode ser realizada pelo estabelecimento de regras, chamadas políticas de segurança.

As ações de um firewall têm basicamente duas regras:

- » Todo tráfego é bloqueado, exceto o que está explicitamente autorizado;
- » Todo tráfego é permitido, exceto o que está explicitamente bloqueado.

Firewalls podem ir além, direcionando determinado tipo de tráfego para sistemas de segurança internos mais específicos ou atuando como um reforço nos procedimentos de autenticação de usuários.

Para entendermos melhor, considere que a complexidade de instalação de um firewall depende do tamanho da rede que ele irá proteger, da política de segurança que a empresa irá implementar, da quantidade de regras que forem implementadas para controlar o fluxo de entrada e saída de informações que passarem por ele. Além disso, é importante termos em mente que ele deverá garantir o grau de segurança desejado em uma rede.

6.3.2 Tipos de firewall – Firewall em forma de softwares

O trabalho de um firewall pode ser realizado de várias formas. O que define uma metodologia ou outra são fatores como critérios do desenvolvedor, necessidades específicas do que será protegido,

características do sistema operacional que o mantém, estrutura da rede e assim por diante. É por isso que podemos encontrar mais de um tipo de firewall.

Elencaremos, a seguir, os mais conhecidos.

6.3.2.1 Filtragem de pacotes (packet filtering)

As primeiras soluções de firewall surgiram na década de 1980, baseando-se em **filtragem de pacotes** de dados, uma metodologia mais simples e relativamente limitada, embora ofereça um nível de segurança significativo.

Pacotes de dados são a estrutura unitária de transmissão de dados ou uma sequência de dados transmitida por uma rede.

Para entendermos melhor: cada pacote de dados possui um cabeçalho com diversas informações a seu respeito, como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, entre outros.

O firewall então analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote (seja para sair ou para entrar na máquina/rede), podendo também executar alguma tarefa relacionada, como registrar o acesso (ou tentativa de) em um arquivo de log, o que criará um histórico de todas as operações que trafegaram em uma rede por meio do firewall.

A transmissão dos dados é feita com base no padrão TCP/IP (*Transmission Control Protocol/Internet Protocol*), que é organizado em camadas.



Figura 6.2 – Filtragem de pacotes.

A filtragem normalmente se limita às camadas de rede e de transporte: a primeira é onde ocorre o endereçamento dos equipamentos que fazem parte da rede e os processos de roteamento, por exemplo. A segunda, onde estão os protocolos que permitem o tráfego de dados, como o [TCP](#).

Importante voltarmos a salientar que a comunicação pela internet é feita, basicamente, por meio de protocolos de comunicação, sendo o TCP (Transmission Control Protocol) um dos mais importantes deles, se não o mais importante. Isso porque o TCP está incluído no conjunto de protocolos que formam o TCP/IP, a base de comunicação via dados de toda a internet.

Para reforçarmos o conteúdo apresentado, apresentamos as principais características do TCP:

- » Garante a entrega de pacotes de dados IP: esta talvez seja a principal função do TCP, ou seja, garantir que os pacotes sejam entregues sem alterações, sem terem sido corrompidos e na ordem correta. O TCP tem uma série de mecanismos para garantir esta entrega.
 - » Executa a segmentação e o reagrupamento de grandes blocos de dados enviados pelos programas e garante o sequenciamento adequado e a entrega ordenada de dados

segmentados: esta característica refere-se à função de dividir grandes arquivos em pacotes menores e transmitir cada pacote separadamente. Os pacotes podem ser enviados por caminhos diferentes e chegar fora de ordem. O TCP tem mecanismos para garantir que, no destino, os pacotes sejam ordenados corretamente antes de serem entregues ao programa de destino.

- » Verifica a integridade dos dados transmitidos usando cálculos de soma de verificação: o TCP faz verificações para garantir que os dados não foram alterados ou corrompidos durante o transporte entre a origem e o destino, verificando o hash dos pacotes.
- » Envia mensagens positivas, dependendo do recebimento bem-sucedido dos dados. Ao usar confirmações seletivas, também são enviadas confirmações negativas para os dados que não foram recebidos: no destino, o TCP recebe os pacotes, verifica se estão OK e, em caso afirmativo, envia uma mensagem para a origem, confirmando cada pacote que foi recebido corretamente. Caso um pacote não tenha sido recebido ou tenha sido recebido com problemas, o TCP envia uma mensagem ao computador de origem, solicitando uma retransmissão do pacote. Com esse mecanismo, apenas pacotes com problemas terão de ser reenviados, o que reduz o tráfego na rede e agiliza o envio dos pacotes.
- » Oferece um método preferencial de transporte de programas que devem usar transmissão confiável de dados baseada em seções, como bancos de dados cliente/servidor e programas de correio eletrônico: ou seja, o TCP é muito mais confiável do que outros protocolos e é indicado para programas e serviços que dependam de uma entrega confiável de dados.

Fonte: definição dada por Júlio Battisti em artigo publicado na JB Livros e Cursos, disponível em http://www.juliobattisti.com.br/artigos/windows/tcpip_p11.asp.

Com base nisso, um firewall de filtragem pode ter, por exemplo, uma regra que permita todo o tráfego da rede local que utilize a porta TCP 80, assim como ter uma política que bloqueia qualquer acesso da rede local por meio da porta TCP 25.

Você deve estar agora se perguntando, mas o que é uma porta no computador?

Para entendermos o conceito de porta, imaginemos um computador, de uma empresa ou pessoal, com conexão à internet.

Você pode, ao mesmo tempo, acessar um ou mais sites, usar o Microsoft Outlook® para ler ou enviar mensagens de e-mail. Ou se estiver em casa, jogar online, digamos, Resident Evil 4®.

Todas as informações recebidas vêm por meio de pacotes de dados que chegam até a placa de rede ou até o Modem DSL, no caso de uma conexão de banda larga doméstica. A pergunta que naturalmente surge é: como o sistema operacional do computador entende para qual dos programas se destina cada um dos pacotes de dados que estão chegando ou saindo? Na chegada de determinado pacote, como o sistema operacional do computador sabe se este pacote é para uma janela específica aberta no meu browser, uma mensagem de e-mail, quem é o destinatário deste e-mail, ou então se não é um comando executado no Resident Evil 4®?

Cada programa trabalha com um protocolo/serviço específico, ao qual está associado um número de porta.

Logo o protocolo TCP/IP possui um conjunto de portas a que ele está associado.

Outro exemplo, o protocolo HTTP, utilizado para transportar as informações de um site que está em um servidor Web até o seu browser, trabalha, por padrão, na porta 80.

Assim todos os pacotes de dados que chegarem destinados à porta 80 serão encaminhados para o browser de internet.

É a existência do conceito de portas que nos permite utilizar vários serviços ao mesmo tempo na internet.

Embora isso também possa representar alguns perigos, é importante ter controle sob o tráfego de dados nas portas TCP. Este controle pode ser obtido por meio da utilização de firewalls, como impedir que programas maliciosos utilizem as portas abertas no computador para atividades mal-intencionadas.

Amplie seus conhecimentos

Caso você queira se aprofundar neste assunto, recomendamos pesquisar e estudar sobre TCP/IP e camadas OSI.

Algumas fontes de pesquisa são:

www.joinville.udesc.br/sbs/professores/erivelto/.../Modelo_TCPIP.ppt
www/usr.inf.ufsm.br/~candida/aulas/espec/Aula_3_Modelo_OSI.pdf
www.telecomhall.com/BR/modelo-de-7-camadas-osi.aspx

6.3.2.2 Filtragens estática e dinâmica

É possível encontrar dois tipos de firewall de filtragem de pacotes.

O primeiro utiliza o que é conhecido como *filtros estáticos*, enquanto o segundo é um pouco mais evoluído, utilizando *filtros dinâmicos*.

Mas o que são estas filtragens?

Na filtragem estática, os dados são bloqueados ou liberados meramente com base nas regras implantadas no firewall, não importando a ligação que cada pacote tem com o outro.

A princípio, esta abordagem não é um problema, mas determinados serviços ou aplicativos podem depender de respostas ou requisições específicas para iniciar e manter a transmissão.

É possível então que os filtros contenham regras que permitem o tráfego destes serviços, mas, ao mesmo tempo, bloqueiem as respostas/requisições necessárias, impedindo a execução completa de uma tarefa.

Esta situação é capaz de ocasionar um sério enfraquecimento da segurança, uma vez que um administrador poderia se ver obrigado a criar regras menos rígidas para evitar que os serviços sejam impedidos de trabalhar, e com isso aumentar os riscos de o firewall não filtrar pacotes que deveriam ser, de fato, bloqueados.

A filtragem dinâmica surgiu para superar as limitações existentes nos filtros estáticos.

Nesta categoria, os filtros consideram o contexto em que os pacotes estão inseridos para “criar” regras que se adaptem aos cenários, permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante um período correspondente.

Desta forma, as chances de respostas de serviços serem barradas, por exemplo, cai consideravelmente.

6.3.2.3 Firewall de aplicação ou proxy de serviços (Proxy)

Você já deve ter ouvido falar em servidor Proxy, um tipo de firewall.

O objetivo principal de um servidor Proxy é permitir que os computadores de uma rede possam acessar uma rede pública, como é denominada a internet, sem que seja necessário ter uma ligação direta com esta, mantendo-se assim o controle do que é acessado.

O **firewall de aplicação**, também conhecido como **Proxy** de serviços (*proxy services*) ou apenas **Proxy**, é uma solução de segurança que atua como um intermediário entre um computador ou

uma rede interna e outra rede, na maioria dos casos uma rede externa – normalmente, a internet.

Geralmente o Proxy é instalado em servidores potentes que se conectam a internet, porque cabe a eles não permitir que seja realizada a comunicação direta entre uma origem e um destino.

Grave bem este diferencial!

O Proxy atua como sendo o procurador das outras máquinas, pois ele é quem faz as solicitações de acesso à web no lugar delas.

A Figura 6.3 ajuda na compreensão do conceito.

Perceba que, em vez de a rede interna se comunicar diretamente com a internet, há um equipamento entre ambos que cria duas conexões: entre a rede e o Proxy, e entre o Proxy e a internet.

Observe:

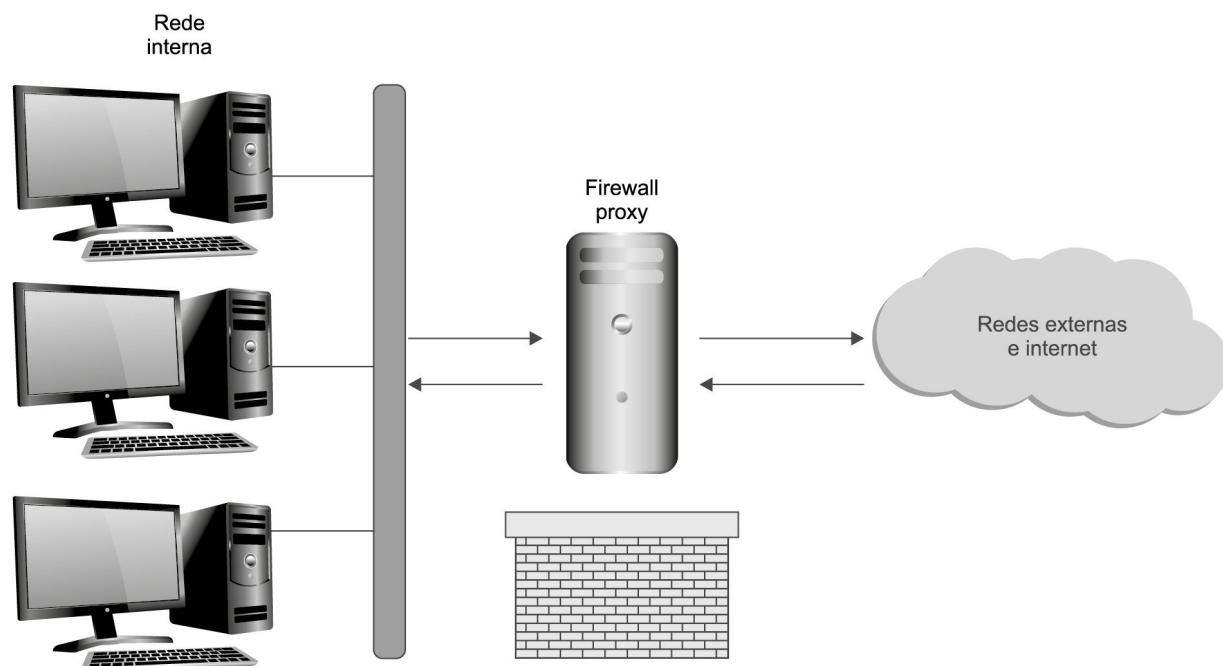


Figura 6.3 – Firewall Proxy.

Perceba que todo o fluxo de dados necessita obrigatoriamente passar pelo **Proxy**.

Desta forma, é possível, por exemplo, estabelecer regras que impeçam o acesso de determinados endereços externos e que proíbam a comunicação entre computadores internos e determinados serviços remotos.

Este controle amplo também possibilita o uso do *Proxy* para tarefas complementares: o equipamento pode registrar o tráfego de dados entre as redes, em um arquivo de log. Desta forma conteúdos muito utilizados podem ser guardados em uma espécie de cache⁶ (uma página da Web muito acessada fica guardada temporariamente no Proxy, fazendo com que não seja necessário requisitá-la e acessá-la no endereço original a todo instante, por exemplo). Alguns recursos podem ser liberados apenas mediante autenticação do usuário.

A implementação de um *Proxy* não é uma tarefa fácil, haja vista a enorme quantidade de serviços e protocolos existentes na internet, fazendo com que, dependendo das circunstâncias, este tipo de firewall exija muito trabalho de configuração para bloquear ou autorizar uma gama muito grande de determinados tipos de acessos.

Normalmente um *Proxy* direciona as solicitações da rede para uma porta específica. Porém, para isso, utilizamos o que é denominado de *Proxy transparente*, ou seja, para os usuários é transparente esta passagem pelo mesmo, mas a mesma fica obrigatória por esta configuração.

Nenhuma solicitação de acesso externo é executada e atendida sem passar pelo *Proxy*.

Amplie seus conhecimentos

Pesquise sobre ferramentas de bloqueio de acesso a sites baseadas na nomenclatura do domínio, tipo SQUID, por exemplo. Você irá com certeza ampliar seu horizonte de ferramentas para implementação de segurança com Proxy.

Pesquise sobre como é colocado em uma rede um Proxy transparente. Olhe as configurações de internet no Painel de Controle de seu computador em casa ou na empresa.

6.3.2.4 Inspeção de estados (stateful inspection)

Tido por alguns especialistas no assunto como uma evolução dos filtros dinâmicos, os firewalls de **inspeção de estado** (*stateful inspection*) fazem uma espécie de comparação entre o que está acontecendo e o que é esperado para acontecer.

Para tanto, os firewalls de inspeção analisam todo o tráfego de dados para encontrar estados, isto é, padrões aceitáveis por suas regras e que, a princípio, serão usados para manter a comunicação estável e segura.

Estas informações são mantidas pelo firewall e usadas como parâmetro para todo o tráfego de dados subsequente.

Para entendermos melhor, suponha que um aplicativo iniciou um acesso para transferência de arquivos entre um computador cliente e um computador servidor.

Os pacotes de dados iniciais informam quais portas TCP serão usadas para esta tarefa.

Se de repente o tráfego começar a fluir por uma porta não mencionada, o firewall pode então detectar esta ocorrência como uma anormalidade, pois o estado da comunicação mudou para um estado não esperado, e assim ele bloqueará este tráfego de dados.

6.3.2.5 Firewalls pessoais

Mas há firewalls mais simples, destinados a proteger o seu computador, seja ele um desktop, um laptop ou um tablet.

São os firewalls pessoais (ou domésticos), que DEVEM ser utilizados por qualquer pessoa.

Felizmente, os sistemas operacionais de uso doméstico ou em escritório normalmente contêm um firewall interno padrão, como é o caso do Linux, do Windows (Firewall do Windows), em todas as suas últimas versões, ou do Mac OS X.

Além disso, é comum desenvolvedores de antivírus oferecerem outras opções de proteção junto ao software, entre elas, um firewall.

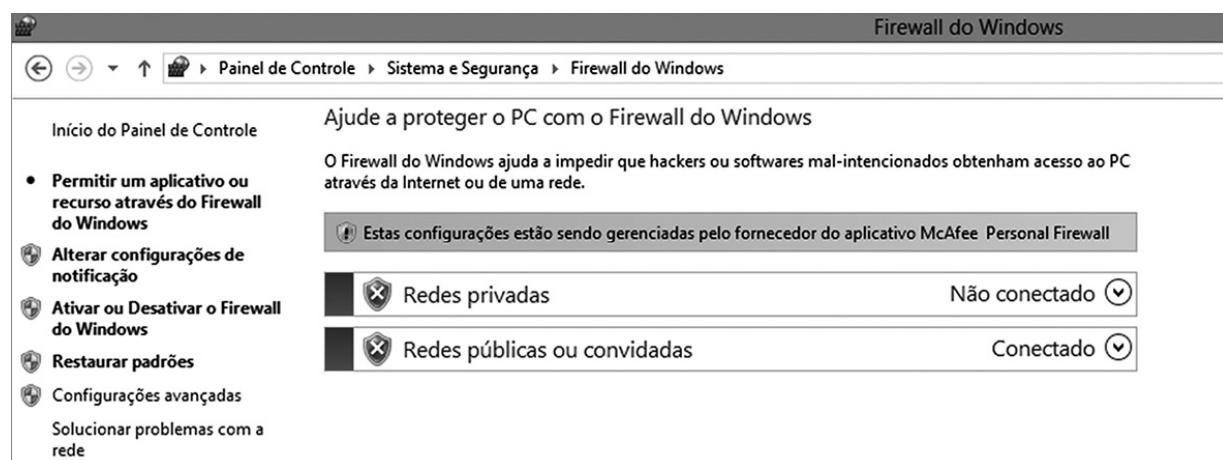


Figura 6.4 – Firewall do Windows.

6.3.2.6 Firewalls de conteúdo

Quando um site é acessado por meio de um firewall de conteúdo (por exemplo, *dnsGuardian*), ele analisa o seu conteúdo em função de uma lista de regras predefinidas e configuráveis pelo administrador do firewall que permitem ou bloqueiam os acessos.

Assim é possível bloquear o acesso a sites indesejáveis, impedir o download de determinados tipos de arquivos ou evitar a propagação de vírus.

Neste item podemos escolher qual é o tipo de conteúdo a ser bloqueado, pois o software utilizado funciona por meio de análise de conteúdo. Selecionei, então, as opções que desejamos bloquear dentre as várias que nos são apresentadas, como pornografia,

chats, games etc., por intermédio da inserção de regras que têm como base palavras-chave na composição da nomenclatura do site: %sports%; %sex%, entre outras.

6.3.2.7 Firewall de hardware

No início deste tema destacamos que um firewall pode ser uma solução de software ou hardware.

Esta informação não está incorreta, mas é necessário um complemento: o hardware nada mais é do que um equipamento com um software de firewall instalado.

É possível encontrar, por exemplo, roteadores ou equipamentos semelhantes a um firewall que exercem a função em questão.

Neste caso, o objetivo é proteger uma rede, normalmente de grandes empresas, com tráfego muito acentuado, ou em grandes volumes, ou com dados muito importantes.

A vantagem de um firewall de hardware é que o equipamento, por ser desenvolvido especificamente para este fim, é preparado para trabalhar com grandes volumes de dados e não está sujeito às vulnerabilidades que eventualmente podem ser encontradas em um servidor convencional (por conta de uma falha em outro software, por exemplo).

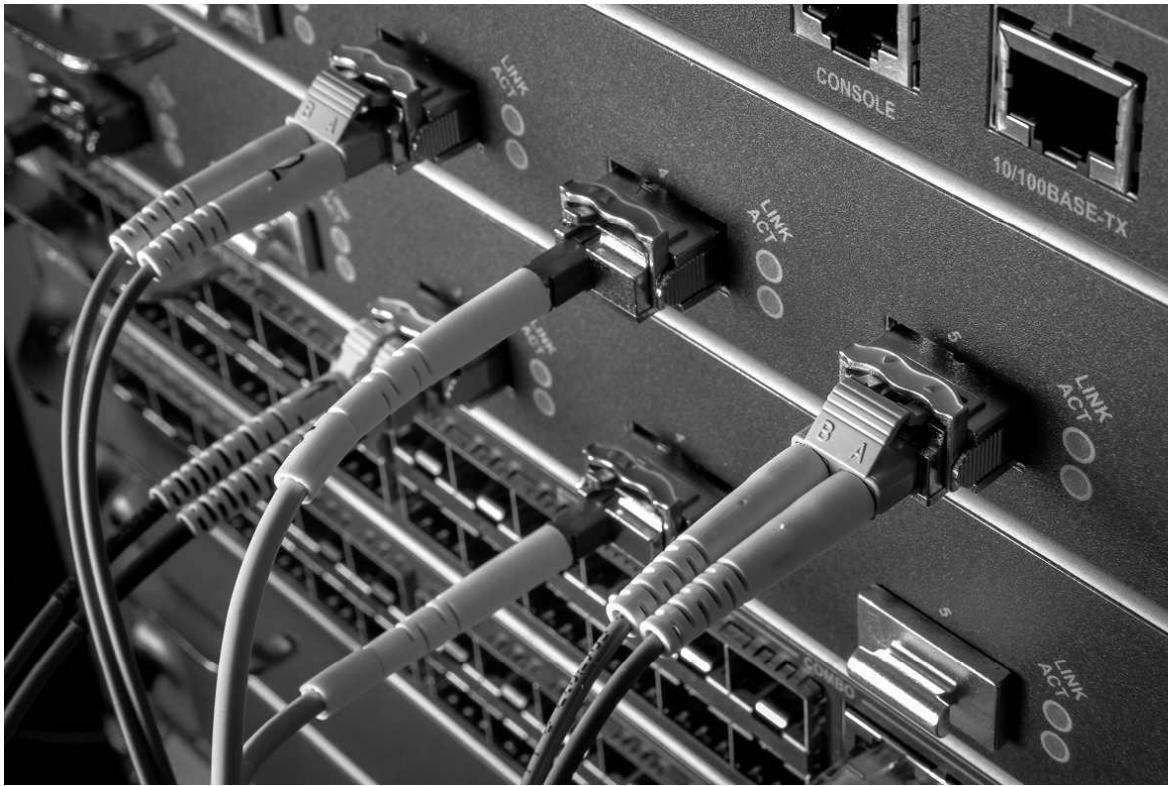


Figura 6.5 – Firewall de hardware.

Outra vantagem quando se utilizam equipamentos desse tipo é que o hardware é dedicado à segurança, às funções de firewall, em vez de compartilhar recursos com outros aplicativos.

Dessa forma, o firewall de hardware pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

Estes equipamentos são chamados de UTM (Unified Threat Management – Gerenciamento unificado de ameaças) e contam com recursos de filtro de pacotes, proxies, antivírus, antispam, concentrador VPN, filtro de conteúdo, IDS/IPS; e em soluções mais robustas, com a capacidade de roteamento avançado, balanceamento de carga de tráfego de rede e extensas possibilidades de relatórios e monitoramento.

A maioria dos roteadores de rede de banda larga domiciliar Wi-Fi disponíveis também contam com algum tipo de aplicação de firewall.

Uma das mais básicas é o controle sobre os computadores que estão habilitados a se conectar na rede. Elas impedem que “sanguessugas” de plantão usem a sua rede Wi-Fi sem permissão, pois necessitam da chave de acesso deste roteador para conectar na sua rede Wi-Fi e acessar a internet.

Amplie seus conhecimentos

Você pode aprender mais sobre a segurança de redes sem fio e firewalls, em sites como:

- » www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm;
- » www.abchost.cz/download/204-4/.../-inspection-firewall.pdf.

6.3.3 Limitações dos firewalls

Você já deve ter notado, mesmo com todos os aspectos destacados, que os firewalls também têm suas limitações, que variam conforme o tipo de solução e a arquitetura e topologia de rede utilizadas.

De fato, firewalls são recursos de segurança extremamente importantes, principalmente em redes de empresas. No entanto, eles não são perfeitos, isto é, não existe nenhuma rede 100% segura, mesmo protegida por um firewall.

Resumidamente, podemos mencionar as seguintes limitações:

- » Um firewall sempre oferece a segurança desejada, desde que esta segurança esteja bem definida e não venha a comprometer o desempenho da rede (ou mesmo de um computador). Situações como esta geram às vezes um custo mais elevado, nos casos em que desejarmos realizar uma ampliação dos recursos tecnológicos de infraestrutura com a finalidade de atender a uma necessidade específica da área tecnológica;

- » A verificação de políticas de segurança e restrições de acesso tem que ser revista periódica e constantemente para não prejudicar o funcionamento de novos serviços e sistemas necessários para uma empresa;
- » Nem sempre novos serviços ou protocolos implementados em uma rede podem estar sendo tratados corretamente pelos proxies já implementados até aquele momento;
- » Um firewall pode não ser capaz de impedir uma atividade maliciosa que se origina e se destina à rede interna (muita atenção a este detalhe, **atividade maliciosa de origem interna à rede**);
- » Um firewall pode não ser capaz de identificar uma atividade maliciosa que acontece por descuido do usuário – quando o usuário, ao clicar em um link de uma mensagem de e-mail, acessa um site falso de um banco, por exemplo (destacamos aqui a questão da interação das pessoas nos problemas de segurança da informação);
- » Firewalls precisam ser “vigiados”, acompanhados permanentemente por pessoas responsáveis e sempre atualizados, porque atacantes experientes podem tentar descobrir ou explorar brechas de segurança;
- » Um firewall não pode interceptar uma conexão que não passa por ele. Se, por exemplo, um usuário acessar a internet em seu computador a partir de uma conexão 3G (para, quem sabe, burlar as restrições da rede), o firewall com certeza não conseguirá interferir e garantir a segurança normal, pois não existirá a passagem deste acesso através do firewall da rede, já que estará sendo realizado um acesso à internet por uma conexão externa à rede, ocorrendo o mesmo fora dos controles existentes no ambiente de rede.

Como você pôde aprender até aqui neste capítulo, os firewalls são soluções importantes de segurança – não é à toa que surgiram na década de 1980 e são amplamente utilizados até os dias de hoje.

Mas, tal como evidenciam as limitações apresentadas, um firewall não é capaz de proteger totalmente uma rede ou um computador, razão pela qual deve ser utilizado sempre em conjunto com outros recursos, como antivírus, sistemas de detecção de intrusos, entre outros.

Utilizar um firewall serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede, mas também a confidencialidade destes dados.

O pensamento que devemos ter é: utilizar um firewall é parte da implementação de segurança da informação, mas não é a segurança em si.

De nada adianta um portão com câmera, na entrada do seu prédio, se além disso não tivermos o pessoal de monitoramento acompanhando. Ou seja, nada funciona sozinho, somente com atuações em conjunto podemos conseguir resultados mais satisfatórios.

Você deve seguidamente se perguntar por que pegamos vírus, por que a internet em alguns casos não tem seu rendimento como esperado em nossa empresa.

A resposta é relativamente simples, segundo [Emerson Alecrim](#):

Nos casos em que temos 100% dos conteúdos liberados perdemos inevitavelmente produtividade por meio de alguns acessos comuns, como Facebook®, YouTube®, Twitter®, entre outros.

Fonte: [Emerson Alecrim](#). Publicado em: 19 fev. 2013. Atualizado em: 19 fev 2013 em <http://www.infowester.com/firewall.php>.

6.3.3.1 Políticas de segurança para firewalls

Um firewall fornece os meios para implementação e aplicação de uma política de segurança no acesso à rede. Este talvez seja o mais importante dos aspectos a considerarmos.

De fato, um firewall fornece controle de acesso de usuários e serviços.

Assim, uma política de acesso à rede pode ser aplicada por um firewall, visto que, sem um firewall, uma política de acesso à rede depende exclusivamente da cooperação e boa vontade dos usuários.

Um site pode ser capaz de depender de seus próprios usuários e da sua cooperação. Entretanto, não pode nem deve depender de usuários da internet em geral.

Existem dois níveis de política de rede que influenciam diretamente na concepção, instalação e utilização de um firewall em uma rede.

A primeira é o que denominamos de política de nível superior. Em outras palavras, trata-se de uma política que define o acesso à rede, contendo as questões específicas que definem quais serviços serão permitidos, quais serviços serão explicitamente negados em uma rede restrita, como esses serviços serão utilizados e quais as condições de exceção a essa política de utilização. Toda regra sempre tem uma exceção.

A seguir temos uma segunda política, de nível mais baixo, que descreve como o firewall irá realmente restringir os acessos e as filtragens dos serviços que forem definidos na política de nível superior.

A política de acesso aos serviços deve se concentrar em questões de uso específico da internet e, principalmente, em todos os acessos a redes do lado de fora.

Esta política deve ser uma extensão de uma política global da organização em matéria de proteção dos recursos de informação na organização.

Para que um firewall seja bem-sucedido, a política de acesso aos serviços deve ser e tem de ser elaborada antes da implementação de um firewall.

Uma política realista é aquela que fornece um equilíbrio entre proteger a rede de riscos conhecidos, enquanto continua a fornecer aos usuários disponibilidade de acesso a recursos de rede.

Se um firewall nega ou restringe serviços, normalmente ele requer que exista a força de uma política de segurança de acesso aos serviços para evitar que os controles de acesso do firewall sejam modificados de forma ad hoc, somente em função de interesses momentâneos ou pessoais.

Outra medida bastante utilizada diz respeito aos filtros por portas e aplicativos. Com eles, o firewall pode determinar, exatamente, quais programas do seu computador podem ter acesso ao link de internet ou não.

As portas de comunicação também podem ser controladas por você, leitor, da mesma forma, permitindo que as portas mais “visadas” pelos malwares sejam bloqueadas terminantemente.

Outra política típica seria permitir algum acesso a partir da internet, mas apenas para sistemas selecionados, como servidores de busca de informação e servidores de e-mail.

Firewalls costumam implementar políticas de acesso de serviços que permitem algum tipo de acesso do usuário a partir da internet para hosts internos selecionados. Esse acesso, contudo, será concedido apenas se necessário e somente se ele puder ser combinado com uma forma de autenticação avançada.

O que desejamos até este ponto do livro é que você, leitor, se acostume com os termos e o objeto política de acessos. É por meio da garantia máxima de segurança de acessos a uma rede, seja interna ou externamente, que buscamos manter a segurança da informação.

Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, como o Windows 8, garantindo a segurança do computador desde o momento em que ele é ligado pela primeira vez, e inclusive com intersecção com um programa antivírus tipo McAfee Internet Security[©].

Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados e entregues ao destino e com que todos os outros fora das regras nunca cheguem ao destino final.

Amplie seus conhecimentos

Você pode aprender mais sobre a segurança de redes sem fio em artigos na internet, pesquise <http://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm#ixzz2sXY0SPFH>.

6.4 Sistemas de detecção de intrusão

Sistemas de Detecção de Intrusão (IDS) são usados para monitorar uma rede ou computadores individuais.

O IDS tem por finalidade detectar uma ameaça ou intrusão na rede.

Pode-se dizer por analogia que um IDS é como se fosse um alarme de uma casa ou de seu carro que toca quando alguém abre a porta.

6.4.1 Mas o que são intrusos?

Intrusos são os invasores (hackers) de um sistema e podem ser classificados em três tipos:

- » **Mascarado** (invasor de fora da rede ou sistema): alguém que não está autorizado a entrar no sistema e o invade para obter privilégios de um usuário legítimo;
- » **Infrator** (invasor de dentro da rede): é um usuário real ou legítimo que não está autorizado a usar determinados recursos, mas os utiliza, ou que está autorizado, mas não os utiliza de forma lícita, sendo considerado mal-intencionado;
- » **Usuário clandestino** (invasor de dentro ou de fora da rede): invasor que toma posse de privilégios de administrador de sistema para escapar das auditorias e dos controles de acesso ou até mesmo para alterar registros de auditorias contra ele.

6.4.2 Tipos de sistemas de detecção de intrusão

Existem dois tipos principais de Sistemas de Detecção de Intrusão: (1) baseados em rede e que monitoram uma rede ou um segmento de uma rede; e (2) baseados em host, isto é, que

monitoram um sistema em particular.

O Sistemas de Detecção de Intrusão em host é instalado em uma determinada máquina (servidor) para avaliar o próprio host. Ele analisa os eventos do sistema operacional, eventos de acesso e eventos de aplicações, monitora as entradas, ou qualquer outra parte que represente tentativa de intrusão. Além disso, bloqueia ataques que não são detectados pelo firewall, como protocolos criptografados. Um IDS deste tipo também acusa uma tentativa suspeita, como um usuário tentando utilizar algo para o qual ele não tenha permissão.

Ele pode ser configurado para observar ataques de crakers, analisar logs de auditoria, alertar um administrador sobre os ataques sendo realizados, proteger os arquivos do sistema, expor as técnicas utilizadas por um cracker e as vulnerabilidades que precisam ser abordadas, corrigidas e, possivelmente, ajudar a rastrear alguns hackers individuais.

Os Sistemas de Detecção de Intrusão baseados em rede (NIDS) são geralmente usados para garantir que usuários não excluem “acidentalmente” arquivos do sistema, redefinem alguma configuração importante ou venham a colocar em risco os sistemas de alguma outra maneira.

Um NIDS é instalado normalmente em um segmento de rede, onde uma base de dados faz as comparações necessárias com os pacotes de rede ou então faz a decodificação e verifica os protocolos de rede.

Os IDS baseados em rede verificam os usuários externos não autorizados a entrar na rede, tentativas de ataques de negação de serviços (DoS) ou roubo de alguma base dados.

Este mesmo tipo de IDS monitora o tráfego de pacotes de rede para descobrir possíveis ataques ou atividades suspeitas, e isso normalmente é feito pela detecção de anomalias e pela identificação de padrões.

O conhecimento é acumulado sobre ataques específicos e como eles são realizados. Modelos desses ataques são desenvolvidos e chamados de assinaturas de ataques. Cada ataque tem uma assinatura, que é utilizada depois para detectar a ocorrência de um novo ataque, caso já tenha ocorrido alguma vez no interior da rede.

Se o volume de tráfego de rede exceder o limite que o sistema IDS suporta, os ataques podem passar despercebidos. Todos os produtos de sistema IDS de qualquer fornecedor têm o seu próprio limite, que devem ser conhecidos e bem compreendidos antes de comprar e configurar o produto de software.

São exemplos de Sistemas de Detecção de Intrusão baseados em rede: RealSecure, NFR e Snort.

São exemplos de Sistemas de Detecção de Intrusão baseados em host: Tripware, Swatch e Portsentry.

Amplie seus conhecimentos

Pesquise e liste as vantagens e desvantagens dos tipos de Sistemas de Detecção de Intrusão Tripware e NFR:

<https://tripwire.dhs.gov/>

www.trtec.com.br/pages/nfr.html

6.4.3 Implementação de sistemas de detecção de intrusão na rede

É comum colocar-se um IDS antes do firewall para impedir que um usuário externo conheça qual é a topologia da rede, e um depois do firewall, em uma área denominada desmilitarizada, para identificar algum ato que o firewall não tenha detectado.

Em instalações de empresas também é normal colocar-se um IDS para detectar ataques advindos da rede interna e, por fim, colocar um HIDS (baseado em host) para aqueles servidores considerados de maior risco a ataques, como o WebServer e os servidores de email.

A Figura 6.6 apresenta uma rede com Sistemas de Detecção de Intrusão antes do firewall e após o firewall, com Sistemas de Detecção de Intrusão de host para os servidores de e-mail e servidor Web.

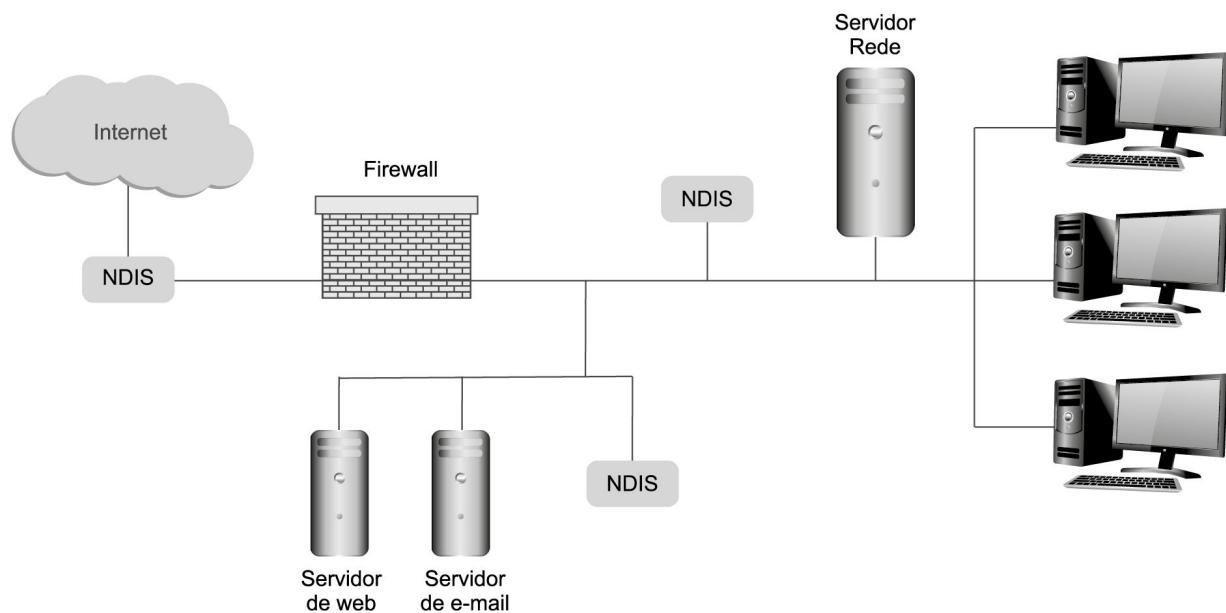


Figura 6.6 – Arquitetura de Sistemas de Detecção com utilização de NDIS e HDIS.

Vamos recapitular?

Neste capítulo aprendemos o que são os firewalls, para que eles servem, quais são suas formas e tipos, assim como sobre a importância da elaboração e existência de uma política de acessos a redes e à internet a partir de uma rede interna, seja ela de uma empresa ou doméstica de banda larga.

Estudamos também o funcionamento dos sistemas de detecção de intrusão em redes. Nos próximos capítulos vamos estudar outras formas bastante importantes no controle de acessos, como as regras de identificação de usuários e criação de senhas de acesso a redes, bancos de dados etc.



Agora é com você!

- 1) A utilização de firewalls abrange quais princípios da segurança da informação?
- 2) Qual tipo de controle controla e bloqueia a entrada de usuários estranhos à rede da empresa?
- 3) Pesquise em sua escola e relacione como estão implementados os firewalls na rede, e faça uma síntese destes processos.
- 4) O acesso a sites como Facebook pode ser bloqueado por um firewall, ou necessariamente temos de ter um software de proxy para este fim?
- 5) Um firewall monitora o tráfego que entra e sai e filtra, redireciona, reempacota e/ou rejeita pacotes de dados?
- 6) Quando queremos monitorar também pacotes criptografados, podemos utilizar um firewall para proteção?

⁶ Cache é uma área temporária para armazenamento de dados de um programa, ou do próprio sistema operacional do computador. O cache de memória funciona como uma extensão da memória, também sendo utilizado para guardar dados temporários e permitir acesso rápido a eles.

Antivírus

 Para começar

Apresentaremos, agora, as ferramentas e as tecnologias que combatem ameaças como vírus, worms e trojans.

7.1 O que é software antivírus?

O software antivírus é um programa de computador que detecta, evita e atua na neutralização ou remoção de programas mal-intencionados, tais como vírus, backdoors, rootkits, trojans, worms, adwares e spywares, entre outros.

Nesse caso, um software antivírus recomendado é o Microsoft Security Essentials.

7.2 Como funciona?

Todo software antivírus possui banco de dados próprio, onde estão armazenadas as informações a respeito das ameaças encontradas nos mais diversos ambientes virtuais, as chamadas assinaturas de vírus.

Essas informações são atualizadas diária e constantemente, a partir de pesquisa e acompanhamento realizados pelos fabricantes dos programas de proteção, buscando e detectando novos vírus lançados na rede mundial. Este é, na verdade, o negócio dos fabricantes de software, que contam, em suas equipes, com hackers altamente especializados nesta tarefa sem fim.

Construindo uma espécie de catálogo com as assinaturas das ameaças, os antivírus rastreiam informações e compararam o comportamento de novos arquivos que acessam o seu computador ou redes com os cadastros existentes em seus bancos de dados.

Dessa forma, eles têm a capacidade de detectar a presença de invasores em sua máquina, o que não significa que eles impeçam a entrada dos já existentes, ou novos, em seu banco de dados.



Nuno Andre/Shutterstock.com

Figura 7.1 – Detecção de vírus.

Outro procedimento comumente utilizado pelos especialistas em antivírus é a chamada análise heurística, cuja função é monitorar as atividades consideradas suspeitas e emitir alertas caso algum programa ou arquivo malicioso tente alterar as configurações do sistema ou de outros arquivos armazenados no computador.

Se você já teve ou tem um antivírus, certamente encontra (em certos casos até com frequência) avisos de que o banco de dados de vírus foi atualizado.

E o que isso quer dizer?

É como se os arquivos que entram na máquina tenham que apresentar um “documento de identidade”. Existe uma lista de “documentos de identidade” no banco de dados do antivírus que indica arquivos que não são permitidos, relacionados em uma lista negra e, portanto, são bloqueados pelos, digamos assim, guardas de segurança do antivírus.

Tanto na proteção ativa quanto nas varreduras completas realizadas pelos antivírus no computador, os mecanismos do antivírus comparam o formato e o comportamento dos arquivos que entram com os que estão registrados em seu banco de dados. Assim, eles são capazes de denunciar elementos perigosos.

Resultado: se um componente é detectado, o antivírus elimina-o para desinfetar o computador.

Apesar de o método de reconhecimento por bancos de dados de vírus ser o método mais utilizado e efetivo para identificar e eliminar vírus, existem outras maneiras de um antivírus encontrar e neutralizar irregularidades no sistema.

Há um processo de detecção de comportamento de vírus chamado análise heurística. Ele monitora constantemente as atividades do computador e entra em ação quando algum programa

tenta modificar configurações do sistema ou arquivos importantes.

7.2.1 Análise heurística

É um conjunto de técnicas para identificar vírus desconhecidos.

Muitos programas, inclusive, utilizam padrão de nomes de vírus específicos para o que é detectado pela heurística.

Um usuário que conhece bem o seu antivírus pode saber quando a análise heurística está agindo para enviar os arquivos suspeitos à companhia produtora do antivírus.

O Norton AntiVirus, por exemplo, chama de “Bloodhound” o que é detectado com essa tecnologia; o NOD32, “NewHeur”, é detectado por análise heurística.



Alphaspirit/Shutterstock.com

Figura 7.2 – Análise heurística.

Uma detecção heurística, por ser genérica, e não sendo específico, apresenta mais chances de indicar como vírus um arquivo analisado, situação em que denominamos o resultado de falso positivo.

Falso positivo é quando o programa antivírus indica que um arquivo é um vírus em razão do seu comportamento. Contudo, trata-se apenas de um arquivo inofensivo cujo comportamento foi interpretado como perigoso ou suspeito.

A técnica de análise heurística do programa é uma tentativa de descobrir se ele contém uma construção típica de vírus de computador.

Na análise heurística do programa antivírus AVG, o elemento principal na análise é um processo especial conhecido como emulador das instruções do processador Intel.

É uma espécie de “computador virtual” que permite a “execução” de um programa ou uma operação do sistema, como inicialização do sistema operacional, a partir do setor de inicialização do disco rígido. Este “executar” é como um simulador, pois não é uma execução efetiva do programa em análise. O programa emulado no computador virtual não é executado diretamente em qualquer sentido da palavra.

O emulador de código recebe suas instruções individuais e, em um modo seguro, imita sua atividade de modo que tudo ocorra em um “computador virtual”, que as instruções não possam afetar de maneira alguma o conteúdo da memória real compartilhada naquele momento por outros programas ou pelo próprio antivírus.

O emulador de código torna totalmente irrelevante o problema da existência de criptografia complexa ou de um código do programa sendo examinado, não completamente transparente.

Quando o programa executa uma atividade significativa no computador real, o emulador das instruções do processador Intel também executa a mesma atividade.

O processo de emulação de código é acompanhado por uma coleta de informações sobre o “significado” do código emulado e por uma avaliação dessas informações. Então o antivírus tenta descobrir se é uma atividade típica de um programa inocente ou, pelo contrário, um comportamento típico de um vírus de computador.

O principal benefício da análise heurística é a capacidade de novos vírus serem detectados, antes mesmo de o fabricante de antivírus poder detê-los e atualizar o seu programa com as novas informações para a detecção desta “novidade”.

Outro método de capturar novos vírus é a verificação de integridade.

Este método, baseado no monitoramento e na avaliação de alterações de programas e nas áreas de sistema do computador, pode identificar e capturar os vírus somente após sua invasão no computador que estava protegido. Isso, infelizmente, pode ocorrer muitas vezes tarde demais.

Entender os princípios da análise heurística também significa entender seus limites.

Antes de mais nada, um fator limitador da análise heurística é que ela não pode detectar vírus programados em linguagem de programação de alto nível (C, Pascal, Basic etc.).

O código de inicialização e as bibliotecas usadas por essas linguagens são bastante extensos e, mesmo que não houvesse nenhum obstáculo técnico impedindo uma emulação profunda desse

programa, para processar um único arquivo o tempo despendido seria de algumas horas a mais do que poderia ser aceitável.

Observe que a análise heurística não é um método utilizado para detectar 100% dos vírus conhecidos ou desconhecidos.

É um dos métodos complementares que aumentam significativamente suas chances de capturar um novo vírus.

Ainda assim, hoje em dia considera-se que a análise heurística é capaz de detectar 70% dos vírus existentes nos arquivos e dos vírus de inicialização, sendo que o número de alarmes falsos (falso positivo) gerados por sua execução é considerado insignificante.

7.2.2 Arquivos em quarentena

Mesmo que pareça estranho, e eu, pessoalmente, fico sempre intrigado e preocupado, os antivírus costumam também fazer com que alguns arquivos sejam enviados para uma espécie de “sistema prisional”.

A chamada quarentena (ou mover para quarentena) é uma opção que a maioria dos antivírus oferece, em determinados casos ou conforme o comportamento suspeito de algum arquivo aos seus usuários.



Figura 7.3 – Quarentena.

Isto acontece porque, durante uma verificação ou varredura do programa de antivírus, alguns programas ou aplicativos encontrados possuem uma conduta suspeita, mas não são identificados como um vírus pelo antivírus ao serem comparados com os dados de vírus em seu banco de dados.

Normalmente, os antivírus informam que existem infecções ou arquivos suspeitos e quais deles devem ser enviados para quarentena. Cabe a você decidir se quer ou não colocá-los em quarentena.

Caso você confirme, estes arquivos são então movidos para quarentena como um meio de penalizá-los.

Nesta área protegida, eles ficam sob monitoramento até que a base de dados do antivírus seja atualizada e, em uma nova varredura, seja detectado o arquivo como um vírus.

Entretanto, como na maioria dos casos os programas de antivírus apresentam o nome de um programa identificado na varredura como perigoso ou suspeito e solicitam a confirmação de que deseja colocá-lo na quarentena, é possível identificar às vezes que o programa indicado não se trata de vírus. Nestes casos, basta recusar a indicação do programa antivírus.

São os chamados “falsos positivos”, isto é, quando o código de um arquivo não comprometedor é identificado, erroneamente, com a mesma sequência de um vírus

Por outro lado, há casos de programas identificados como suspeitos que podem realmente comprometer o registro do sistema ou até o funcionamento de aplicações e jogos.

Chamamos sua atenção, leitor, para sempre identificar o programa considerado perigoso. Assim, você evitará colocar em quarentena programas sem qualquer problema que foram erroneamente identificados pelo antivírus.

Quando um arquivo verificado durante a varredura é encontrado no banco de dados do programa antivírus, o programa automaticamente o remove do sistema.

7.2.3 Falso positivo e falso negativo

Quando um antivírus examina um arquivo, ele sempre responde, internamente, a uma pergunta implícita: “Esse arquivo é um vírus?”

A resposta pode ser positiva (“sim, é”) ou negativa (“não, não é”).

Quando um antivírus dá uma resposta positiva incorretamente, pois o arquivo não é um vírus, diz-se que ocorreu um “falso positivo”. Quando o antivírus deixa escapar um vírus, o termo é “falso negativo”.

Se você sabe que o arquivo sugerido para a quarentena é um vírus ou desconfia de um arquivo e o antivírus não o está detectando, o melhor procedimento é enviá-lo para análise do fabricante de antivírus. Esta atitude não só ajudará a pesquisa de proteção contra vírus. Você também terá, com certeza, um retorno do fabricante, para remover ou ficar seguro quanto a este arquivo.

A maioria dos programas de antivírus possui opções em seus menus para realizar esse procedimento.

Fique de olho!

Enquanto houver brechas no funcionamento de equipamentos eletrônicos, haverá gente disposta a burlar seus esquemas e agir de forma mal-intencionada. Portanto, quem deve estar atento para não sair perdendo sempre é o próprio usuário.

A quarentena tem como objetivo isolar as possíveis pragas digitais. Ela não tem como finalidade proteger arquivos legítimos e seu computador contra infecção.

Em programas antivírus, outra tecnologia de detecção utilizada chama-se HIPS (Host Intrusion Prevention System), que é uma tecnologia para analisar o comportamento dos programas em execução.

Ela também é conhecida como “behaviorblocking”.

Com esta tecnologia, os antivírus fazem a verificação se um programa em execução realiza atividades suspeitas, como envio de e-mails em massa (spam), download de muitos arquivos, entre outros comportamentos que podem indicar a possibilidade de existência de um vírus.

Ela é diferente da análise heurística. Enquanto esta última analisa um arquivo em si e simula sua execução, ela analisa somente os programas em execução.

Lembrando que, apesar de todos os métodos existentes, nenhum programa antivírus consegue detectar 100% das ameaças.

Quando um computador já está infectado, é evidente que o antivírus falhou.

No entanto, veremos quantos casos de vírus foram detectados, barrados ou eliminados por um antivírus utilizado no computador até então.

É muito comum encontrarmos este cenário: o seu computador está infectado e você instala outro programa antivírus. Ele, então, remove os vírus que estavam no computador, não detectados pelo programa anterior.

Portanto, concluir que o segundo programa antivírus é melhor é uma conclusão equivocada e é importante evitá-la. Tudo pode ser uma questão de frequência da atualização do antivírus, pois eles estão sempre com novos elementos maliciosos em suas listas.

Antigamente os programas antivírus removiam e protegiam somente contra vírus, e nós precisávamos ter ainda instalados outros programas para remover spywares, ou programas específicos contra trojans etc.

Isto não é mais nossa realidade. Hoje, tudo está integrado em um único programa antivírus. Aplicativos antispywares são cada vez menos comuns. Você tem em um programa antivírus proteção e detecção total contra todos os tipos de ameaças, sejam trojans, spywares, adwares, vírus etc.

7.2.4 Arquivos executáveis

Muitas vezes, as pessoas ou usuários mais leigos assustam-se ao ouvirem falar em arquivo executável.

Vamos deixar claro aqui o que é um arquivo executável: são arquivos que, ao serem abertos, realizam comandos. Eles não são necessariamente um vírus ou uma ameaça. Grande parte dos programas de sistemas em empresas, e até mesmo em seu computador pessoal, são arquivos executáveis. O próprio sistema operacional tem seus programas executáveis.

As extensões comuns para esses arquivos são EXE, BAT, SCR, DLL e COM.

Quando você estiver em dúvida sobre um arquivo deste tipo, execute a verificação do programa de [antivírus](#) nestes arquivos antes de abri-los.

Se você pesquisar sobre antivírus para fazer download, sempre escolha os mais conhecidos, pois, hoje em dia, já existem crackers usando estes procedimentos de as pessoas realizarem download para enganá-las com falsos softwares antivírus. Assim, você instala um “antivírus” e deixa seu computador mais vulnerável ainda aos ataques.

Antivírus gratuitos normalmente não possuem atualização de seus bancos de dados com a mesma frequência, qualidade e abrangência que os softwares pagos. Não oferecem, portanto, uma cobertura contra ameaças mais amplas.

“Não utilize software pirata!”

7.2.5 Assinaturas de vírus

Não, você não vai fazer uma assinatura para ter um vírus!

Assim como a sua assinatura de nome identifica a sua identidade como pessoa, a assinatura de um vírus é o que o antivírus utiliza também para identificar que uma ameaça digital está presente em um arquivo.

A assinatura é geralmente um trecho único do código do vírus.

Procurando por esse trecho, o antivírus pode detectar o vírus sem precisar analisar o arquivo inteiro.

7.2.6 Síntese das funções dos programas antivírus

- » Identificar e eliminar uma boa quantidade de vírus;
- » Analisar os arquivos de downloads;
- » Verificar continuamente os discos rígidos do computador e mídias removíveis de forma transparente ao usuário;
- » Procurar e detectar vírus, spywares e trojans em arquivos anexados aos e-mails;
- » Criar um disco de verificação (disco de boot) que poderá ser utilizado caso algum vírus seja mais esperto e anule o antivírus instalado no seu computador. Normalmente utilizamos um CD *não regravável para a gravação deste disco de boot*.

Amplie seus conhecimentos

Visite os sites dos dois maiores produtores de antivírus e aprenda mais sobre soluções e novidades quanto à proteção contra vírus:

<http://www.symantec.com/pt/br/>

<http://www.mcafee.com/br/>

7.2.7 A importância do antivírus

Pesquisas indicam que, do total de usuários de internet no país, 15,5% não utilizam programas antivírus, o que corresponde a 14 milhões de usuários desprotegidos. Tais usuários estão expostos, inclusive, à possibilidade de hackers utilizarem sua máquina, como computador zumbi, em ataques a sites ou roubo de dados bancários.

Infelizmente, apesar de saberem de todas as vantagens de ter um programa antivírus, são poucos os brasileiros que se dispõem a pagar por uma solução que proteja realmente seu computador.

Seja por falta de informação sobre as vantagens ou pelo simples fato de acharem que estão protegidos com alguns antivírus gratuitos, muitos acreditam nesta pobre ilusão.

Quem já teve problemas com dados roubados, cartões clonados, sabe qual é o valor que um bom antivírus tem.

Hoje os antivírus contam com fortes ferramentas, como o “antiphishing”, que evita que o usuário entre em sites falsos e tenha seus dados pessoais “pescados” (disto surgiu o termo phishing). Eles contam também com ferramentas de “busca segura”, que analisam um site listado em uma busca na internet, antes mesmo de você entrar nele e ser infectado por malwares.

Além de outras proteções que guardam seus dados e os protegem, prevenindo que você acidentalmente os envie a sites e computadores desconhecidos.

Vamos recapitular?

Neste capítulo você aprendeu sobre o que é um antivírus, como ele funciona, seus métodos e técnicas utilizadas na detecção e identificação de códigos maliciosos.

Você também foi informado sobre o que significa colocar um arquivo suspeito em quarentena, quais métodos são utilizados para identificar comportamentos de vírus, o que é a análise heurística, assim como sobre a importância de possuir instalado um programa antivírus dentro do contexto da Segurança da Informação.



Agora é com você!

- 1) Explique a diferença entre antivírus e firewall.
- 2) Análise heurística é:
- 3) Colocar em quarentena significa:

- 4) Códigos maliciosos escritos em linguagem “C” podem ser identificados por um programa antivírus?
- 5) Explique com suas palavras o que é um falso positivo.

8

Segurança em Dispositivos Móveis

 Para começar

O crescimento do número de equipamentos móveis (por exemplo, telefones celulares, smartphones, tablets, notebooks, coletores de dados, entre outros) conectados a redes e sistemas corporativos demanda que sejam definidos controles e padrões para que não se perca a flexibilidade fantástica de sua utilização. Ao mesmo tempo torna-se fundamental que sejam mantidas as garantias dos princípios da segurança da informação.

Tem-se exigido, assim, a utilização de métodos, regras e controles dos profissionais de segurança da informação, assim como o comprometimento dos usuários destes equipamentos empresariais de forma consciente e comprometida. Neste capítulo vamos nos dedicar a conhecer as principais ameaças da utilização destes recursos e os procedimentos recomendados para a manutenção da segurança da informação corporativa.

8.1 Introdução

O armazenamento de dados corporativos em dispositivos móveis se tornou uma grande preocupação para os gestores de tecnologia da informação (TI) nas empresas de médio e grande porte.

Para ilustrar o momento em que vivemos, segue uma pesquisa sobre o assunto:



Figura 8.1 – Dispositivos móveis.



Exemplo

Uma pesquisa encomendada pela Check Point com cerca de 800 profissionais de TI dos EUA, Canadá, Reino Unido, Japão e Alemanha, em junho de 2013, revelou que 79% das empresas entrevistadas registraram alguma ocorrência de segurança envolvendo dispositivos móveis de seus funcionários nos últimos 12 meses. Fontes: <http://blog.segr.com.br/pesquisa-revela-alta-incidencia-de-problemas-de-seguranca-com-celulares-corporativos/> e em <http://segbit.com.br/pesquisa-revela-alta-incidencia-de-problemas-de-seguranca-com-celulares-corporativos.html>.

O problema mais comum é o roubo ou a perda de dispositivos móveis, principalmente smartphones, com informações corporativas. Em seguida está a infecção destes equipamentos por códigos maliciosos, por meio de redes Wi-Fi inseguras e navegação em sites não seguros.

A maior preocupação dos gerentes de TI não é quanto ao fato de existirem pessoas mal-intencionadas, mas sim que seus funcionários sejam descuidados. Pesquisas recentes apontam que em 66% dos casos são os próprios funcionários os principais responsáveis pelos incidentes de segurança da informação nas empresas.

A máxima “*o aparelho não é meu, é da empresa*”, por mais absurda que pareça, é o primeiro aspecto a ser considerado. O fato de não ter despendido valores para adquirir o equipamento faz com que muitos funcionários não tenham o devido cuidado e preocupação com os dispositivo que teriam se fossem de sua propriedade e tivessem gastado para adquiri-los.

Cada dia mais populares e acessíveis, os smartphones e tablets estão na mira dos hackers.

8.2 Utilização de dispositivos móveis

Os usuários não procuram ficar bem informados acerca dos riscos que correm e, como afirmamos, eles não têm com estes dispositivos móveis os mesmos cuidados que normalmente possuem com computadores tradicionais, seja uma estação de trabalho ou um notebook.

O sistema operacional Android, desenvolvido pelo Google® para smartphones, é hoje o alvo preferencial dos mal-intencionados, principalmente por ser o mais popular do mundo e por sua natureza de ser de código aberto, o que possibilita a instalação de aplicativos de qualquer origem.



Exemplo

“As pessoas ainda encaram os celulares como se estivéssemos nos anos 1940, ou seja, como se fossem simples objetos destinados apenas a fazer ligações”, afirmou o diretor sênior de segurança móvel da McAfee, John Dasher, durante o evento Focus 11, promovido pela empresa em Las Vegas, em 2011.

Na realidade, se observarmos, os usuários de smartphones e tablets não se dão conta de que aquele pequeno aparelho que carregam no bolso é um computador, com as mesmas vulnerabilidades dos PCs tradicionais, ou até mais graves do que elas em certos casos.

O perigo, porém, não deve se limitar a celulares e tablets. Ele se estende aos mais variados tipos de dispositivo, desde televisores até aparelhos de ginástica (alguns equipamentos de ginástica, em academias sofisticadas, permitem acesso à internet), que começam a ser equipados com sistemas operacionais completos e acesso à internet.

A Cisco (fabricante de equipamentos de conectividade) já previa que até 2015 haverá 15 bilhões de dispositivos conectados, ou cerca de dois por habitante do planeta.

Para exemplificar, vejamos algumas notícias publicadas na *Folha de S.Paulo* online:



Exemplo

Um caso de malware no Android foi descoberto e revelado por um fabricante de antivírus, a Symantec:

Aproveitando-se do fato de o aplicativo do serviço de vídeo Netflix estar disponível apenas para um número limitado de aparelhos com Android em seu início de operações, mal-intencionados distribuíram na rede uma versão falsa do mesmo, com o objetivo de roubar dados de assinantes. Fonte: <http://www1.folha.uol.com.br/fsp/tec/tc2610201115.htm>

Assim como acontece com os computadores, os ataques direcionados aos dispositivos móveis ainda são baseados em grande parte nas técnicas de engenharia social, estudadas anteriormente.

Nessa prática, os hackers usam diversos recursos para fazer com que o usuário clique em um link. Este, por sua vez, acaba por direcioná-lo para uma página infectada de um site e instala algum malware no aparelho.

8.2.1 Smartphones e códigos maliciosos

A incidência de vírus para smartphones ainda não pode ser considerada alarmante. No entanto, já é significativa o suficiente (em particular para o Google Android®) para que as pessoas passem a tratar os smartphones como tratam os computadores pessoais e estações de trabalho da empresa. A maior preocupação é com a disseminação de aparelhos corporativos e, principalmente, sua utilização fora do ambiente de trabalho.

Um dos maiores problemas do sistema operacional Android® é o crescente número de aplicativos (Apps) maliciosos, que é facilmente identificado por um usuário.

Estes Apps são identificados principalmente por especialistas em segurança, que os reportam ao Google, que então os remove dos serviços disponíveis para o Android.

A recomendação dos especialistas é que se utilizem somente aplicações do serviço oficial de Apps e Google Play.

Para sua segurança, recomendamos:

“Desmarque a opção Permitir a instalação de aplicativos de fontes desconhecidas”, porque assim somente as aplicações permitidas pelo Google Play serão instaladas no seu equipamento com o sistema Android.

8.2.2 Tablets e códigos maliciosos

Com um incontável número de fabricantes desenvolvendo grande quantidade de tipos de tablets (*Motorola Xoom, Apple iPad, Samsung Galaxy Tab, HP TouchPad, Dell Streak 7, RIM PlayBook*, etc.) em cima de diferentes sistemas operacionais (*Android, iOS, WebOS, BlackBerry Tablet OS*), é evidente que devemos nos preocupar mais com a segurança destes dispositivos. Os ataques de códigos maliciosos possivelmente aumentarão.

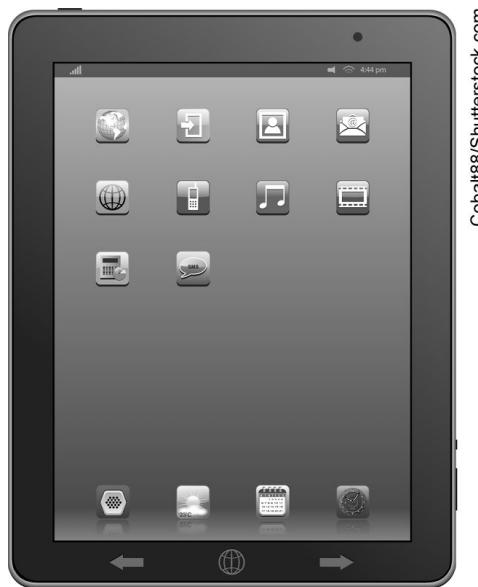


Figura 8.2 – Tablets.

Apesar de existirem falhas de segurança já documentadas em todos os sistemas operacionais, os hackers têm voltado sua atenção para o sucesso de vendas dos iPads e demais tablets, com sistema operacional [Android](#).

Todos sabem das restrições da Apple aos seus sistemas e hardwares, com o iPad isso não é diferente.

A quantidade de aplicativos desenvolvidos para o iPad é gigantesca. Porém, antes de serem disponibilizados para os usuários, eles são enviados à Apple, que durante algumas semanas os submeterá a testes e análises dos códigos. Somente depois de aprovadas pela equipe técnica, portanto, estarão disponíveis para download.

Durante este processo de validação da Apple, qualquer parte do aplicativo que possa causar risco ao equipamento, como mau funcionamento e vírus, é identificada, tratada e, em seguida, os criadores são informados. Entretanto, dependendo das anomalias encontradas, o aplicativo pode ser rejeitado.

Apesar de parecer um processo um tanto quanto burocrático e lento, é com essa política que a fabricante garante que seus produtos funcionarão sempre de maneira segura e satisfatória.

Conforme os desenvolvedores ganham confiança por um bom [desenvolvimento](#), a Apple prioriza a análise das aplicações dele, agilizando o processo. Porém nada elimina a passagem por esta análise.

Com todo este controle é difícil, aliás, muito difícil, criar códigos maliciosos e colocá-los na loja de aplicativos da Apple (App Store). Ainda assim muitos usuários ficam insatisfeitos com esta política, pois várias destas aplicações têm de ser pagas, e as pessoas não querem pagar por elas, principalmente no Brasil. Passam, então, a utilizar o chamado JailBreak (*fuga de presos*).

O JailBreak é um iOS (sistema operacional do iPhone, do iPad e do iPod Touch da Apple) modificado, cuja instalação vai contra os termos de garantia dos equipamentos Apple.

Ao instalar o iOS, passa a ser possível instalar qualquer aplicativo no iPad sem a necessidade de acessar a loja de aplicativos. Consequentemente, o usuário assume os riscos de causar danos irreversíveis ao aparelho e deixa de contar com a garantia do produto.

A primeira versão do JailBreak saiu para o iPhone (tanto iPhone quanto iPad usam o mesmo sistema operacional).

Este sistema foi criado por um grupo de [hackers](#) que, por incrível que pareça, são contra a pirataria. Eles apenas não aceitam que o usuário de um equipamento da Apple não possa ter controle total sobre o produto que adquiriu.

Com essa “*filosofia*”, não são disponibilizados os arquivos do sistema modificados, mas sim a ferramenta para que o usuário os modifique conforme suas necessidades.

Para tentar evitar a evolução e o uso do JailBreak, a Apple informou publicamente que sua utilização é uma prática ilegal e passível de penalidades legais. Entretanto, a organização Electronic Frontier Foundation (EFF) é a favor desta prática. Para esta organização, o usuário tem o direito de modificar o próprio equipamento da forma que achar mais conveniente, afinal ele o comprou.

Com a utilização do JailBreak, os usuários tornaram-se vítimas dos *atacantes mal-intencionados*, pois os aplicativos que são disponibilizados fora da loja de aplicativos da Apple não possuem qualquer controle de qualidade e podem perfeitamente conter códigos maliciosos mascarados dentro deles.

Diferentemente da Apple, a [Google™](#) possui a política de liberdade para tudo o que produz. Desta forma, praticamente todos os seus produtos possuem uma versão paga e uma grátils (inclusive de excelente qualidade) equivalente.

No caso do Android Market (mercadinho), as aplicações são publicadas diretamente pelo usuário e, diferentemente da Apple, não passam por uma rigidez de controle de qualidade, o que é muito bom para quem desenvolve, assim como para os mal-intencionados. Contudo, não há qualquer garantia de qualidade. Pode-se falar, assim, que há certa facilidade em desenvolver e publicar aplicações na Android Market, que já vem sofrendo com vírus publicados e distribuídos para seus usuários.

Outro fator muito importante e preocupante nos sistemas Android é que eles são baseados no Linux e obviamente de código aberto. Com isso os usuários podem ter acesso total ao sistema com a

conta de superusuário (root).

Uma vez tendo esse acesso, é possível efetuar qualquer modificação desejada no código do programa, como a liberação de uso de compartilhamento de 3G, funções de Wi-Fi, atualização da versão do Android antes das operadoras disponibilizarem uma nova versão “customizada” dela etc.

Aproveitando-se dessa característica e liberdade de criação e alteração, diversos trojans já foram desenvolvidos com o intuito de modificar o núcleo do sistema operacional para executarem suas funções sem nenhuma percepção do usuário.

E você, leitor, bem despreocupado com seu tablet!

8.2.3 Segurança em tablets

Os tablets geralmente usam um adaptador de rede sem fio com baixo consumo de energia para se conectarem à internet e, por meio dela, às suas redes corporativas.

Com um Tablet pode-se acessar a Web, e-mails etc.

Considerando que o equipamento trabalha com baixas taxas de consumo de energia, a intensidade do sinal wireless utilizado normalmente é baixa.

Sendo assim, é relativamente fácil provocar um nível de interferência (utilizando um “Acess Point” ou até mesmo um laptop) suficiente para impedir que um Tablet possa se conectar ao local correto, induzindo-o, então, a se conectar a um ponto de acesso “mal-intencionado” (rogue access point).

Além disso, algumas vezes é possível realizar um ataque de negação de serviço denominado “ping DoS”, que irá consumir todos os recursos disponíveis do Tablet, deixando-o extremamente lento, impraticável de se trabalhar.

Você deve se perguntar qual o objetivo destes ataques, não é?

Da mesma forma que nos computadores, o objetivo é ter acesso a senhas, a dados não autorizados etc.

Os ataques a Tablets ocorrem em número muito menor se comparados aos ataques a computadores, Contudo, isso é apenas uma questão de tempo. Oferecemos, portanto, seis recomendações para uso seguro dos Tablets:

- 1) Coloque senha de acesso (no iPhone e iPad há a opção de formatação em caso de erro em dez tentativas);
- 2) Não desbloqueie seu aparelho (no caso do iPad – JailBreak);
- 3) Acesse apenas sites confiáveis;
- 4) Não instale aplicativos suspeitos;
- 5) Desabilite o Bluetooth (habilite com senha apenas quando for fazer transferência de dados);
- 6) “*Não é extremamente necessário*”, mas se possível instale um software antivírus.

Não é por modismo que as empresas consideram os dispositivos móveis um tema “*difícil*” ou “*muito difícil*” na área de TI e, principalmente, no tocante à segurança da informação.

Apesar dos vários fatores positivos que são decorrentes desta utilização crescente dos dispositivos móveis nas empresas, entre os quais destacam-se a mobilidade, a agilidade e o acesso mais fácil às informações, esse movimento também é motivo de preocupação para as empresas, em especial quanto à segurança dos dados corporativos.

Funcionários que trabalham com informações corporativas em dispositivos pessoais acabam levando informações sigilosas para fora da empresa, pois os equipamentos os acompanham fora do ambiente de trabalho. Eles permitem, assim, a possibilidade de

transferência de dados, dão oportunidade para a ocorrência de furto de informações, a manipulação de dados sigilosos, a ocorrência de infecções de vírus ou mesmo ataques hackers quando em uso fora da rede da empresa.

A eventual perda desses dispositivos móveis, em decorrência de um assalto ou extravio, pode ainda permitir que terceiros tenham acesso a rede virtual da empresa, e-mails corporativos e particulares, senhas de acesso a rede e aplicações, agenda de contatos corporativos, entre outros.

A solução que as empresas mais têm adotado é a implementação de um conjunto de recursos de software que traga garantias do cumprimento das regras de acesso às informações e os níveis de segurança exigidos, bem como ofereça aos seus usuários (funcionários) soluções simples e rápidas de operação destes equipamentos.

Isso pode ser feito a partir de um diagnóstico das redes corporativas das empresas para oferecer soluções sob medida. Desse maneira, permite-se a integração dos smartphones e Tablets ao ambiente corporativo, por meio da virtualização das aplicações de acesso a rede (as chamadas máquinas virtuais, VMs), e o uso de ferramentas que bloqueiem qualquer tentativa de desvio de informações.

8.2.4 Segurança em conexões WI-FI

Como nosso tema de estudo é a mobilidade, torna-se uma prioridade para a questão da segurança destacar que estes equipamentos (tablets, smartphones, iPads e iPods) normalmente são vistos em aeroportos, bares, cibercafés e restaurantes, ou outros locais que possuam alguma disponibilização de redes sem fio para acesso à internet.

Neste ponto destacamos que existe uma questão importante de segurança.

Como estamos nos conectando a redes abertas, a existência de uma chave de acesso não traz garantia alguma. Fornecida a todos que desejam conexão, estas redes não possuem nenhum protocolo de segurança que impeça que os seus dados sejam capturados por completo.

Você pode, ao enviar um e-mail, ser interceptado nesta rede. Além de pessoas mal-intencionadas terem acesso à sua mensagem, seus dados de acesso poderão ser também capturados.

Isso se dá porque uma rede Wi-Fi pública funciona mais ou menos como um walkie-talkie. Ela opera em frequências de rádio públicas, que podem ser sintonizadas por qualquer um que se encontra nas proximidades do local em questão.

Para ter total privacidade ao acessar contas de e-mail, serviços de mensagens instantâneas, redes sociais e demais websites, uma possibilidade é utilizar uma conexão criptografada (estudaremos mais detalhes sobre criptografia neste livro).

Este processo de criptografia evita que as informações de login, por exemplo, sejam enviadas como texto puro, dificultando assim o trabalho de hackers e outros mal-intencionados.



Halfpoint/Shutterstock.com

Figura 8.3 – Conexão WI-FI.

Devemos também observar outro detalhe: esse tipo de conexão criptografada possui a URL (endereço da página na barra de endereços do browser) das páginas iniciadas com “HTTPS”, que indica um protocolo seguro, em vez de “HTTP”.

Outro ponto importante é certificar-se de que a conexão continue criptografada até o fim.

Vale chamar atenção para sites como o Facebook, que criptografam o login do usuário, mas depois do acesso se tornam uma navegação insegura.

Para saber e pesquisar, existem aplicativos como o DroidSheep, que é muito usado por invasores mal-intencionados. Eles são extremamente nocivos para um consumidor inocente.

O DroidSheep monitora, nos ambientes a que nos referimos, as conexões realizadas e informa os “logins” de sites como o LinkedIn, Gmail, Yahoo e, até mesmo, o Facebook.

As senhas na realidade não podem ser vistas juntamente com o login. Mas o mal-intencionado pode acessar uma conta em andamento e obter os dados da mesma ao seu alcance.

Para impedir que estes fatos aconteçam o melhor é utilizar aplicativos de segurança para smartphones e tablets, que podem ser obtidos nas lojas de aplicativos dos mesmos. Ou então ainda recomendamos ter um antivírus no aparelho.

Ao checarmos nosso e-mail em um equipamento móvel, devemos fazer o login no navegador-padrão do aparelho e nos certificarmos que a conexão é criptografada.

Em caso de um cliente de e-mail como o Outlook, é importante verificarmos se a criptografia está habilitada nas especificações de contas, sejam elas POP3 ou IMAP e SMTP.

8.2.5 Acessando remotamente uma Rede com Tablets

Quando um usuário se conecta a uma rede sem fio corporativa, ele deve ter acesso à internet somente por meio de um serviço de proxy. Dessa forma, permanecerá isolado da rede corporativa e dos recursos disponibilizados por ela.

A autenticação será realizada a partir de uma base única de usuários, seguindo os mesmos procedimentos já estudados para identificação, autenticação e autorização do usuário nos recursos, sejam eles de rede, de acesso a aplicações e bancos de dados e utilização de e-mail, ou de acesso às aplicações disponibilizadas na internet.

Outra alternativa com as redes sem fio é a conexão a um determinado computador da rede por meio da utilização da área de trabalho remota.

A área de trabalho remota conecta, na verdade, dois computadores por meio de uma rede ou da internet.

Uma vez conectado, aparecerá a área de trabalho do computador remoto e o acesso a todos os programas e arquivos estará liberado. Estaremos, assim, trabalhando no computador em que se conectou.

Após acessarmos este computador, teremos de executar todos os passos normais de identificação e autenticação, assim qualquer acesso que seja realizado, ele estará acontecendo neste computador que você se conectou, seguindo as regras corporativas normais de segurança.

Algumas empresas liberam o acesso de tablets por meio da área de trabalho remota, utilizando o serviço de Terminal Server da Microsoft.

Mas desde já destacamos que é um processo que sobrecarrega a rede e muitas vezes torna-se lento demais para possibilitar a execução de um trabalho produtivo, principalmente se as aplicações forem acessadas por meio do Terminal Server (TS).

Para melhorar esta performance são utilizados servidores de TS para atender exclusivamente a esta demanda de conexões.

8.2.6 Conclusão sobre redes sem fio

O tráfego de informações em redes sem fio ainda é objeto de estudo quanto às melhores soluções para a segurança da informação.

A facilidade de se trafegar dados dispensando a necessidade de conexão a qualquer tipo de rede por meio de cabos tem atraído cada vez mais usuários e empresas em todas as partes do mundo.

Entretanto, o fato é que, em termos práticos, este meio de comunicação ainda não está totalmente protegido de invasões e fraudes, realidade que está diretamente relacionada ao desenvolvimento dos padrões de comunicação dessas redes.

Um exemplo simples é o padrão WEP (Wired Equivalent Privacy) que predomina nas redes de banda larga DSL, mas que já demonstrou possuir falhas graves de segurança.



Tyler Olson/Shutterstock.com

Figura 8.4 – Acesso remoto sem fio em rede pública.

Recentemente especialistas descobriram meios de acessar a chave utilizada em sua criptografia quebrando a segurança deste padrão. Logo em seguida, apresentaram diversas ferramentas disponíveis na internet e capazes de romper a segurança de redes sem fio que utilizam o protocolo de segurança denominado WEP.

Concluindo nossa abordagem, destacamos que as redes sem fio têm vulnerabilidades com origem na sua própria concepção e em seu padrão de segurança.

É por esta razão que os atuais fornecedores de produtos trabalham na atualização e em melhorias na segurança destes sistemas de transmissão e comunicação de dados.

Amplie seus conhecimentos

Uma notícia extremamente recente para você entender como os ataques já estão acontecendo em função também da utilização de dispositivos móveis.

Novo golpe envolvendo o WhatsApp para desktop é identificado.

O popular aplicativo de mensagens instantâneas WhatsApp, adquirido pelo Facebook recentemente pelo alto valor de US\$ 19 bilhões, foi mais uma vez alvo de cibercriminosos, que não perderam tempo e criaram um novo ataque de spam afirmando que a versão desktop do aplicativo móvel já está sendo testada.

Os engenheiros da Trend Micro encontraram uma amostra de spam que menciona a compra do WhatsApp pelo Facebook e também informa que a versão desktop do WhatsApp já se encontra disponível para Windows e Mac. A mensagem fornece um link para o download da suposta versão, que foi detectada como TROJ_BANLOAD.YZV, comumente utilizado para baixar malwares bancários.

Recomendamos você a ler as notícias variadas sobre ataques e ameaças a dispositivos móveis apresentadas no site a seguir. Fonte: <http://adrenaline.uol.com.br/seguranca/noticias.html?bc=45>.

Vamos recapitular?

Neste capítulo falamos sobre como os dispositivos móveis estão sujeitos a ataques de pessoas mal-intencionadas, conheceu os riscos que envolvem os sistemas operacionais destes equipamentos e como eles acabam acontecendo.

Falamos também sobre os cuidados a serem tomados na utilização de equipamentos móveis corporativos e que, ao utilizá-los, somos os responsáveis por eles tanto dentro como fora do ambiente da empresa, o que é importante principalmente por pertencer à empresa e possivelmente conter dados sobre seu trabalho e corporativos em certos casos.

A atenção com a segurança contra extravio e roubo destes equipamentos deve ser levada em consideração sempre que um funcionário recebe os mesmos para melhoria e flexibilidade de seu desempenho profissional. É muito importante lembrarmos que acessos em lugares públicos estão sujeitos a fácil interceptação dos dados que você está acessando ou enviando.

Também é importante o destaque que demos a algumas pequenas ações como colocar senha no seu iPad para protegê-lo de acessos indevidos em caso de furto ou roubo.



Agora é com você!

- 1) Um Firewall num dispositivo móvel impede o roubo de informações? Explique.
- 2) Um tablet tem menos risco de ser invadido por vírus que um smartphone?
- 3) Pesquise e faça uma lista de 3 (três) softwares antivírus para smartphones.
- 4) O que pode acontecer com seus dados se utilizar um tablet na rede de um aeroporto para enviar e-mails?
- 5) Se você tem um smartphone, pode conectá-lo à rede sem fio da empresa com os mesmos recursos que você tem em sua estação de trabalho (PC)?

9

Controles e Processos de Segurança

 Para começar

Aprenderemos, agora, procedimentos e processo recomendados para a segurança da informação, tais como classificação de dados, realização de cópias de segurança e utilização de mídias removíveis. Estudaremos também algumas técnicas para proteger dados pessoais ou dados em uma rede.

Se não realizarmos cópias de segurança de nossos dados, qualquer problema físico ou lógico (um vírus, por exemplo) pode simplesmente levar à perda de todas as informações armazenadas. Imagine o quanto isto pode ser impactante em uma empresa.

Como o valor dos dados não é único em uma empresa nem em um computador pessoal, explicaremos as razões de ser feita a classificação de dados.

9.1 Introdução

Realizar backups dos arquivos existentes em um computador é um meio eficiente de evitar perdas irreparáveis de informação. Entretanto, backups desnecessários não são considerados o mais correto em razão de alguns fatores, como:

- » Capacidade da mídia digital utilizada para a cópia de segurança;
- » Vida útil da mídia utilizada;
- » Dados desnecessariamente copiados (por exemplo, arquivos temporários de internet);
- » Multiplicidade de mídias desorganizadas (fitas ou DVDs sem identificação);
- » Tempo consumido para realização do processo de backup (grande quantidade de dados salvos todos os dias).

Em um primeiro momento, vamos comentar sobre o que deve ser salvo, o que é, realmente, importante para um usuário ou uma empresa. Vamos também entender um aspecto da segurança da informação, que é a classificação dos dados, em razão do seu valor para o negócio ou para um usuário.

9.2 Classificação de dados

É importante reconhecer qual informação é fundamental para uma empresa e atribuir a ela um valor.

A lógica de atribuir um valor aos dados deve ser capaz de permitir mensurar a quantidade de recursos que devem ser utilizados para protegê-la, porque nem todos os dados têm o mesmo valor para uma empresa ou para um usuário isolado.

Uma boa forma para a classificação dos dados é organizá-los de acordo com as implicações resultantes em caso de perda ou divulgação inapropriada.

Quando uma empresa classifica seus dados de acordo com a importância das implicações resultantes em caso de sua perda, estamos decidindo na realidade quais controles de segurança e prioridade de segurança deveremos ter para os diferentes tipos de dados existentes em uma instalação de TI de uma empresa.

A razão principal de realizarmos a classificação dos dados é indicar o nível de confidencialidade, integridade e disponibilidade requerido para cada tipo de dado.

Cada classificação deverá ter procedimentos específicos para seu acesso, uso, backups e deleção, inclusive.

Por exemplo, todos os procedimentos necessários para planilhas eletrônicas criadas e que não sofrem processos de atualização desde sua criação nem serão atualizadas no futuro (i.e., tabelas fixas) têm necessidade de realização de cópias de segurança, completamente diferentes dos dados existentes no banco de dados utilizado por uma aplicação de faturamento (notas fiscais) que diariamente estão sendo criados ou até excluídos novos dados.

Logo a interpretação destes dados classificados deverá com certeza ser diferenciada. Dados que não são estruturados em sistemas de aplicação e que também não são atualizados em nenhum momento não possuem a mesma necessidade de serem geradas cópias de segurança, com o mesmo nível de preocupação que as bases de dados de sistemas de aplicação.

Outro aspecto a ser considerado quando classificamos dados é que podemos, dependendo da classificação de um dado, exigir chaves específicas para acessá-los, manter registros para auditoria dos acessos e alterações (arquivos de log), com monitoramento inclusive diário, e até exigir a existência de cópia destes dados em papel, se necessário, dependendo da forma de operação de negócios da empresa.

Os especialistas utilizam classificações em diversos modelos e tipologias para as empresas no país.

Vamos seguir um modelo internacional, e mais utilizado hoje, que considera informações de negócios e inclusive informações militares.

Lembrando sempre que a classificação dos dados depende muito do tipo de negócio da empresa e dos objetivos e metas dela.

A sensibilidade dos dados à sua perda (*i.e.*, o quanto de prejuízo ao negócio implica sua perda ou exposição indevida) é o que define sua classificação.

Empresas do setor privado são geralmente mais preocupadas com a integridade e disponibilidade dos dados que a maioria das organizações militares no mundo.

Uma empresa pode optar por usar como classificação de dados os tipos confidencial e público, enquanto outra empresa pode optar por usar top secret, secreto, confidencial, sensível e não

classificado.

Normalmente os níveis de sensibilidade, do mais alto para o mais baixo, para empresa privada cujo negócio é principalmente comercial, são:

- » Confidencial.
- » Privado.
- » Sensível.
- » Público.

Uma vez que os tipos de classificação são definidos, a empresa precisa desenvolver os critérios que vai usar para decidir quais informações entram em cada classificação.

Sugerimos, por experiência, que seja utilizada como critério a lista de parâmetros a seguir:

- » Utilidade dos dados (quem define esta utilidade é quem utiliza o dado na empresa);
- » Valor do dado (qual a importância financeira do dado para a empresa);
- » Idade do dado (refere-se a data e a hora da última modificação do dado);
- » O nível do dano que poderia ser causado se os dados forem divulgados;
- » O nível de dano que poderia ser causado se os dados forem modificados de forma não autorizado ou corrompidos;
- » Leis, regulamentos ou responsabilidades que a empresa tem sobre a manutenção e proteção dos dados junto a órgãos regulamentadores, como a Agência de Vigilância Sanitária;
- » Quem deve acessar estes dados (dados que são restritos a alta direção, por exemplo);
- » Quem deve fazer a manutenção desses dados;
- » Onde devem ser mantidos e armazenados esses dados;

- » Quem está autorizado a reproduzir esses dados;
- » Quais dados exigem que se tenha uma espécie de rótulo ou alguma marcação especial.

Portanto, depois que temos o esquema de classificação definido e todos os dados são classificados, o que foi determinado através da análise dos dados por critérios como os que sugerimos, o próximo passo é especificar como os dados inseridos em cada classificação devem ser tratados.

Tabela 9.1 – Classificação de dados

Classificação	Definição
Sensíveis	Requerem cuidados especiais para garantir a sua integridade, protegendo-os de alterações ou deleção não autorizada.
Confidenciais	Para serem utilizados apenas na empresa. São os dados que têm proibida a sua divulgação por leis e regulamentos.
Privados	São as informações pessoais para uso dentro de uma empresa. A divulgação não autorizada dos mesmos pode afetar adversamente os funcionários da empresa.
Públicas	Todos os dados que não se incluem nas categorias anteriores. Sua exposição não autorizada não é interessante, mas não causa nenhum impacto aos negócios da empresa.

Nesta tabela, observamos que cada classificação possui necessidades diferentes e necessita de requisitos de segurança diferentes também. Inclusive, como veremos, no tocante à realização de backups.

Hoje ainda há empresas que tratam de seus dados de forma indiscriminada, sem qualquer distinção de classificação, criando políticas de segurança como se seus dados fossem de um tipo só. Isto afeta diretamente a execução de cópias de segurança e as próprias políticas de segurança são normalmente fracas nestas situações.

Se você não identifica distinção entre os dados que estão em uma rede de computadores e seus sistemas e estações de trabalho, como tratar a segurança destes dados com critério. Todos são tratados da mesma maneira? No mínimo estaremos desperdiçando recursos para manter a segurança, ou não estaremos mantendo a segurança de forma adequada para dados que deveriam receber um tratamento especial.

Quando os dados são inadvertida ou intencionalmente expostos a pessoas que não deveriam ter acesso a essa classificação de dados, as empresas devem possuir processos em andamento para destruir ou restaurar os dados e reduzir os prejuízos desta exposição indevida.

Bancos, em particular, têm exigências rigorosas para relatar divulgações imprevistas de dados sensíveis. Trata-se, assim, de padrões a serem seguidos e especificados pelas suas várias entidades e órgãos governamentais reguladores das operações deste tipo de negócio.

Os desenvolvedores de sistemas de informação de uma empresa devem ser capazes de comunicar-se não só com o pessoal de segurança da área de TI, mas com executivos do lado do negócio da organização. São eles que compreendem os requisitos para o seu negócio e o tipo de classificação que desejam de seus dados.

Todas as partes interessadas numa empresa devem estar conscientes da importância e dos critérios de classificação de dados para que obtenha sucesso na utilização e controle desta classificação.

É importante destacar que os dados existem sempre em três estados básicos: *em repouso, em processo e em trânsito*.

Em todos estes três estados, os dados exigem soluções técnicas para a manutenção da sua integridade, confidencialidade e disponibilidade, como também para sua classificação. Logo, os princípios aplicados na classificação destes dados devem ser o mesmo em cada um destes estados.

Em outras palavras, se os dados são classificados como confidenciais, eles têm a necessidade de continuarem confidenciais, independente do estado em que se encontrarem: **em repouso, em processamento ou em trânsito**.

9.3 Backups – cópias de segurança

O que é um backup?

Backup é uma cópia dos dados em um computador ou em um sistema que será armazenada em uma mídia magnética removível como fitas magnéticas, DVDs ou discos rígidos removíveis. É importante destacarmos que sua finalidade é permitir a restauração destes dados em caso de ocorrência de uma perda total ou parcial de algum deles no computador ou na rede onde se encontram.

Backup é um termo inglês cujo significado é cópia de segurança.

O backup contém os dados no estado em que se encontravam no momento (data e hora) em que foi realizada esta cópia.

Um processo de backup ajuda a proteger os dados de uma perda acidental em decorrência de uma falha de hardware ou nos meios magnéticos de armazenamento, ou contra perdas ou alterações indevidas, acidentais ou inclusive mal-intencionadas.

Mas o que é e como deve ser feito um processo de backup?

Relembrando que o objetivo principal de um backup de dados é restaurar estes dados no caso de perda ou, simplesmente, de necessidade de retornar dados para o estado em que estavam em uma data e hora anterior e específica, por algum outro motivo operacional ou de negócios. Ele é utilizado também para indicar a existência de uma cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento simultaneamente.

Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada e os dados perdidos respostos em seu lugar de origem.

O backup é valorizado por quem já perdeu alguma vez informações importantes e não teve a possibilidade de recuperá-las. Uma das situações mais desesperadoras, portanto, é perder documentos digitais e não haver a possibilidade de recuperá-los, sendo necessário, então, gerar ou criar todos ou uma série de documentos novamente.

O backup é um dos procedimentos para a manutenção da segurança da informação altamente recomendável em razão da frequência com que incidentes ocorrem, quando se perde muita ou as vezes toda a informação, seja por ações não intencionais de um usuário, ou por acessos maliciosos e não autorizados. Ou seja, em decorrência de mau funcionamento de sistemas ou hardwares.

Mas o processo de backup, mesmo sendo realizado por aplicações específicas do sistema operacional ou programas independentes, deve ser executado obedecendo a critérios, para que seja um processo organizado.

Necessitamos realizar a criação de uma arquitetura para backup, e isso é uma tarefa relativamente complexa em ambientes de rede, em virtude da heterogeneidade dos elementos que os compõem.

Novamente observe que o objetivo principal é a realização do backup dos sistemas em produção, a fim de os manter disponíveis caso seja necessário a recuperação dos dados armazenados.

Para que este objetivo fundamental seja atingido diversos fatores técnicos e organizacionais devem ser considerados. E, como não poderia deixar de ser, temos a questão da concorrência dos recursos de processamento de uma rede, pois há muitos usuários realizando processos de forma constante durante o horário de operação de negócios da empresa.

A infraestrutura necessária para backup é composta por diversos elementos de tecnologia, como drivers, mídias, o servidor de backup, as interfaces de rede, a rede de dados, o meio de armazenamento do backup e, inclusive, o hardware dos usuários que efetuam o backup.

É necessário analisar estes recursos sob três pontos de vista: arquitetura, dimensionamento e sua utilização.

Quando falamos de arquitetura, significa que os recursos tecnológicos devem ser combinados ou integrados de forma que a utilização aproveite sua máxima capacidade, assim como permita um grau de flexibilidade na utilização dos mesmos.

A infraestrutura para termos um backup corporativo deve ser montada desde o início, possibilitando as mais diferentes realidades de operação, tecnologias e recursos. Ela deve também estar pronta para ser adaptada continuamente, conforme mudam e crescem as necessidades dos servidores, volumes e tecnologias utilizadas, e que viram objeto da cópia de segurança.



Figura 9.1 – Backup em fita.

Quando falamos em dimensionamento, estamos considerando dentro dos critérios para a execução de backup a quantidade de volumes necessários para comportar os arquivos copiados, assim como as necessidades de tecnologia para os servidores, tipos de mídias, volumes de dados crescentes e necessidade de meios de armazenamento e guarda destas cópias.

Estes recursos devem ser configurados de modo a oferecer uma capacidade de vazão suficiente para que os volumes de backups sejam realizados dentro das janelas de tempo definidas e estes mesmos recursos sejam reutilizados e continuamente atualizados, adaptados e integrados com novos recursos que se fizerem necessários, em razão do crescimento das aplicações de novos sistemas e novas tecnologias utilizadas na empresa.

Uma característica que deve ser considerada como um fator extremamente importante é que um processo de backup tem de ser fluxo contínuo, ele não pode sofrer interrupções, perda de continuidade ou paradas de espera, além de consumir mais recursos computacionais, apresenta também riscos de integridade e qualidade da cópia de segurança.

Não existe a possibilidade de um processo de backup iniciar, pausar ou parar e continuar novamente. Um backup captura os dados em um determinado momento, não sendo possível iniciá-lo, pausar e continuar, pois o momento já mudou o valor dos mesmos, assim como em uma fotografia, se iniciarmos e pararmos para depois continuar o momento retratado já não será mais confiável nem retratará um momento específico. Da mesma forma, a interrupção e o reinício de um backup iria capturar e copiar os dados em momentos e estados completamente diferentes, ou seja, parte dos dados em um momento e parte em outro momento, logo sem integridade garantida.

É necessário que todos os fatores envolvidos no backup corporativo sejam entendidos e levados em consideração.

Estes critérios também devem considerar importante a classificação dos dados e sempre serem realizados no que se denomina de janela de backup.

O que é uma janela de backup?

A janela de backup é a quantidade de tempo disponível e sua localização no calendário (data e hora) para realizar a cópia de um determinado volume de dados, e que deve ter uma programação de execução e de dimensionamento para a execução do backup.

Entretanto, quando lidamos com um backup corporativo, não pode existir somente uma janela de backup, que sempre é relacionada a um evento de calendário (dia, semana, mês etc.).

A determinação de uma janela está vinculada ao ciclo da atualização de dados das aplicações de sistemas da empresa.

Lembrando que sempre que necessário será utilizado um backup para restabelecer a condição operacional de um sistema, a partir de uma imagem destes dados em um momento no tempo anterior.

É normal que, em algumas aplicações, isto signifique que existirá uma certa perda de dados entre a cópia armazenada no momento da execução do backup e um momento atual.

Temos de considerar que existem aplicações que funcionam, no que se convencionou chamar de 24 x 7, ou seja, 24 horas por dia, 7 (sete) dias da semana. Isto significa que são aplicações que estão sempre gerando novos dados ou alterando os seus dados continuamente.

Para estes casos a programação dos backups deverá sempre buscar a determinação de o mesmo ser executado em horários de baixo nível de atualização dos dados, buscando minimizar a perda para um nível que possa ser considerado aceitável.

9.3.1 Políticas de backup

Um backup deve ser programado para capturar e preservar um volume de atualizações que represente a menor perda de dados aceitável entre a sua execução e o momento seguinte.

Como podemos concluir, não existe um conceito absoluto de quando um backup deve ser realizado.

Considerando estes fatores, existe o que se denomina de política de backups, que busca analisar e especificar como poderemos, com os backups, preservar a disponibilidade das aplicações por meio da segurança dos dados armazenados.

É normal existir a tendência natural de alinhar esta política de backup com eventos de calendário, como dias e semanas, mas não é o mais correto.

Considerando-se os sistemas que funcionam 24 x 7, para estes não existe o conceito de dia.

Em sistemas que funcionam mundialmente na internet tampouco.

Observe bem que em sistemas comerciais (varejo) que funcionam 24 x 5 podem ser necessários pelos menos dois backups no período de um dia, uma vez que ninguém se arriscará a perder um dia inteiro de vendas e faturamento, como um exemplo extremo, mas lembrando que sempre é possível ocorrerem desastres.

Por fim, a criação desta política de backup com estabelecimento de frequência, datas e horários está diretamente vinculada aos tipos de backups que utilizaremos.

Isto pode variar em uma política de backup de acordo com o tipo de sistema de aplicação objeto de backup, assim como depende dos recursos tecnológicos disponíveis na empresa, entre eles mídias de armazenamento (fitas), servidores de backup, volumes de dados, e da distribuição física destes recursos e dos recursos de pessoal técnico disponíveis.



Figura 9.2 – Segurança física de backups.

Importante salientar que na realização de um backup, após gerar fitas com cópias de segurança, estas devem ser guardadas em local apropriado e classificadas caso haja a necessidade de busca e recuperação.

Para isso normalmente as empresas possuem cofres especiais à prova de fogo e localizados fora da área geográfica da TI, como garantia extra de segurança.

9.3.2 Tipos de backup

Vamos considerar neste livro quatro tipos ou métodos para execução de backup de dados em um computador ou em uma rede de computadores.

9.3.2.1 Backup geral de cópia

Este backup realiza a cópia de todos os arquivos selecionados.

Ele é útil caso você queira fazer cópia de todos os arquivos entre os tipos de backups normal e incremental, que veremos a seguir, pois ela não afeta essas outras operações de backup.

Mas, no caso de sistemas e dados corporativos em rede, este tipo de backup é demorado, lento e consome muitos recursos, o que faz com que ele seja executado somente em uma frequência muito pequena, ou quando da execução do primeiro backup de uma instalação de rede.

9.3.2.2 Backup diário

Copia todos os arquivos selecionados em uma determinada classificação de dados que foram modificados no dia de execução do backup diário.

9.3.2.3 Backup incremental

Um backup incremental copia somente os arquivos criados ou alterados desde o último backup normal ou incremental e os marca como arquivos que passaram por backup.

Se optarmos por uma combinação de backups normal e incremental, precisaremos do último conjunto de backup normal e de todos os conjuntos de backups incrementais para restaurar os dados.

Observe que esta necessidade de processar diversas cópias de segurança para restabelecer um determinado momento dos arquivos é consideravelmente mais demorada que a restauração, realizada com uma única cópia dos dados. Entretanto, o backup incremental é um processo com certeza mais rápido em sua execução e permite a criação de janelas de tempo de curta duração para sua execução.

9.3.2.4 Backup normal

Um backup normal copia todos os arquivos selecionados e os marca como arquivos que passaram por backup.

Com backups normais, só é necessário a cópia mais recente do arquivo ou da fita de backup para restaurar todos os arquivos selecionados e copiados.

Geralmente, o backup normal é executado quando criamos um conjunto de backup pela primeira vez. Porém, este tipo de backup deve ser realizado entre períodos mais longos, desde que exista uma garantia de integridade da mídia de armazenamento da cópia realizada. É normal os analistas de segurança da informação realizarem a duplicação das fitas de backup como garantia extra contra a possibilidade de ocorrência de problemas físicos de acesso e aproveitamento das cópias realizadas.

O backup dos dados que utiliza uma combinação de backups normal e incremental exige menos espaço de armazenamento e é o método mais rápido tanto na execução quanto na recuperação. Entretanto temos de realizar periodicamente este backup completo.

No caso de executado o backup normal completo em intervalos muito longos, é possível que a recuperação de arquivos seja difícil e porque o conjunto de backup pode estar armazenado em vários discos ou fitas e ser muito extenso.

Fique de olho!

Backups são importantes, mesmo no computador pessoal. Mas guardar as mídias que contêm as cópias em segurança e em ambiente controlado é tão importante quanto executar e verificar se a execução ocorreu normalmente e ficou correta.

De nada adiantam backups realizados sem controle e acompanhamento. Pesquise sobre programas para execução seletiva de backups, como backups incrementais, e conheça como são realizados e operados estes programas e/ou sistemas.

9.4 A utilização de mídias removíveis

A popularização dos pen drives, com sua praticidade e flexibilidade, está exigindo que as empresas adotem políticas de segurança para evitar que sejam abertas possibilidades de violação dos princípios básicos de integridade, disponibilidade e confidencialidade.

Tais dispositivos medem centímetros, possuem apenas uma microplaca de circuito e um chip de memória. Ainda assim não podemos subestimar o potencial de perigo que eles podem representar.

Hoje, um simples pen drive pode abrigar até 64 gigabytes de informação. Esta capacidade significa o equivalente ao conteúdo aproximado de 16 DVDs, a alguns milhares de músicas, filmes completos, milhares de fotos, se pensarmos somente em entretenimento. Por outro lado, em uma visão mais danosa, estes 64 gigabytes podem representar mais de 30 milhões de registros de clientes de uma empresa.

Cada vez menores, mais potentes e mais baratos, estes chips de memória multiplicam-se e são a maneira mais simples e rápida de armazenar e transportar arquivos de um computador para outro.



Marius G/Shutterstock.com

Figura 9.3 – Pen drive 1.

Não é mais necessário, portanto, entender de conexões em rede entre duas máquinas.

Basta espetar um pen drive em uma das entradas USB do computador, fazer a cópia física das informações e depois abri-las em qualquer outro aparelho que tenha uma entrada USB, como computadores, televisões, entre outros.



Exemplo

“A possibilidade de copiar dados em pen-drives não seguros, iPods e computadores de mão, entre outros aparelhos, tem representado um tormento para os esforços de segurança”, diz Larry Ponemon, presidente do Ponemon Institute, empresa americana que pesquisa vazamentos de dados e segurança da informação.

Os pen-drives já são o segundo meio mais utilizado para transportar documentos e dados corporativos para fora da companhia, segundo pesquisas da empresa de segurança digital McAfee.

Apesar das precauções tomadas para regular a utilização de pen drives nas empresas, como eles são cada vez menores, está cada dia mais fácil perdê-los. Com isso, dados de milhões de clientes de uma empresa podem ficar expostos de um momento para outro.

Não basta simplesmente radicalizar e proibir a utilização de pen drives por meio do bloqueio de portas USB, por exemplo, afinal a multiplicidade de tipos de computadores em uso em uma empresa não permite mais que se recorra a uma solução tão simples e retrógrada.



Exemplo

A gigante da aviação Boeing também revelou, no ano passado, ter sido vítima do roubo de 320.000 arquivos de documentos confidenciais por um funcionário que agiu por cerca de dois anos e utilizou memórias portáteis como aliadas. Fonte: <http://www.universitario.com.br/noticias/n.php>.

Hoje possuímos softwares que gravam no servidor a data que um usuário conectou um pen drive em algum computador da empresa e qual conteúdo foi copiado. Veja isso, você não sabia mas

está sendo controlado. Isto é segurança da informação.

A proibição radical em nada resolve, pois funcionários necessitam dos recursos de mobilidade. Neste contexto, os pen drives têm significativa importância para, no caso de necessitar de uma simples apresentação de um projeto, a mesma ser transferida de um computador para outro em outra instalação.

Se você perdesse o seu pen drive hoje, o que teria nele?

Muita gente carrega informações pessoais dentro deles, como currículos, fotos da família e dos amigos, boletos de contas a pagar e arquivos em geral. Outras chegam ao absurdo de salvar senhas e informações sigilosas nesses dispositivos. Portanto, temos de ter meios de proteger também os dados que foram gravados no pen drive, independente de serem da empresa ou não.

Por outro lado, os pen drives são considerados um dos principais transmissores de vírus, worms e trojans, entre outras pragas digitais, porque as pessoas os utilizam em computadores de lan houses e de amigos, que, às vezes, não possuem antivírus.

Agora tanto do ponto de vista da gravação quanto da leitura dos dados de um pen drive, temos duas preocupações com a utilização deste tipo de mídia em uma rede de uma empresa:

Para uso pessoal, existem programas como o [ProtegPen](#) (gratuito). Além de ser simples, este programa permite que, quando o pen drive for espetado em um computador de uma lan-house ou em qualquer outro computador, nada possa ser gravado nele, evitando assim que vírus se instalem no dispositivo.

O [ProtegPen](#) funciona como um cadeado para proteger determinado dispositivo móvel, já que com ele é possível que seja permitida, ou não, a entrada de arquivos. O programa é extremamente simples de usar, pois possui apenas uma janela e

demanda o uso de no máximo três botões. Tem como característica o armazenamento no formato NTFS (New Technology File System). Nesse caso, se o pen drive utilizar outro formato de gravação como [FAT32](#), será necessário converter o armazenamento do dispositivo.

Outro programa utilizado para evitar cópias (edição) e deleção de arquivos de um pen drive é o [USB Write Project](#) (também gratuito).



Figura 9.4 – USB Write Project.

Estes programas permitem que seja realizado o bloqueio e desbloqueio simples de gravação em um pen drive.

Chamamos atenção que esta é uma solução para proteger o pen drive. Não se trata de uma solução para uma empresa que deseja evitar que seus arquivos sejam copiados para um pen drive. É uma

boa solução para ser utilizada se você, leitor, for levar um pen drive para um amigo copiar as músicas do computador dele para o seu dispositivo.

Basta protegê-lo contra gravação e permitir a leitura dos arquivos, assim seu amigo poderá copiar. Mas se existirem vírus no computador dele, não será possível que se instalem em arquivos do pen drive.

Para uma empresa, existem softwares que permitem que os administradores de rede bloqueiem completamente o uso de pen drives (opção radical demais). Uma outra alternativa seriam os softwares que configuram os computadores para que somente leiam esses dispositivos, com varredura completa deles por programas antivírus, ou criptografem todos os dados, bem como monitorem, bloqueiem e registrem os arquivos que são enviados para eles, ou lidos nesses dispositivos.

O mais adequado, portanto, é:

- » Garantir que vírus que possam existir em um pen drive não sejam instalados no computador onde ele foi conectado;
- » Garantir que vírus não se instalem em um pen drive;
- » Impedir cópias não autorizadas de dados em um pen drive;
- » Impedir a transferência de softwares ou arquivos não autorizados para o computador ou para arquivos da rede e vice-versa;
- » Em alguns casos, impedir a leitura sem identificação e senha de arquivos de dados gravados em um pen drive.

Além disso, a maioria desses softwares cria registros de todos os dados que se movem de e para as bases de dados da empresa, permitindo que os administradores de rede e segurança de informação criem políticas que não necessariamente restrinjam completamente o uso do dispositivo de mídia removível ou

dispositivo sem fio, e sim permitam a visibilidade completa da atividade dos mesmos e do conteúdo trafegado de e para estes dispositivos.

No que diz respeito ao vazamento de informações de empresas, as estatísticas mais atualizadas nos sinalizam a seguinte distribuição (práticas indevidas dos funcionários que colocam em risco muitos dados corporativos):

Tabela 9.2 – Distribuição dos vazamentos de informação

A distribuição dos perigos em uma empresa	
Cópia de informações confidenciais da empresa em pen drives	51%
Compartilhamento de senhas com colegas de trabalho	46%
Perda de equipamentos portáteis de armazenamento de dados	39%
Envio de documentos da empresa em anexo para e-mails pessoais	33%

Fontes: McAfee e Ponemon Institute

Amplie seus conhecimentos

Pesquise na área de segurança da TI de sua escola ou empresa sobre os procedimentos de controle de mídias removíveis e softwares utilizados para este controle.

Identifique claramente quais restrições podem ser realizadas por estes softwares. Procure ver em suas aulas práticas ou em seu trabalho como é encarado o uso de pen-drives. Tente utilizar um pen-drive na porta USB e copiar algum arquivo do computador do laboratório e do pen-drive para o computador. Veja se o computador faz também uma varredura com programa antivírus.

Faça um teste de segurança. Vá a uma loja e peça para o vendedor tentar ler, em um computador de consulta de preços, por exemplo, o seu pen-drive e veja se o computador faz também uma varredura com programa antivírus.

Vamos recapitular?

Neste capítulo estudamos o que é classificação de dados, a importância e o porquê de ela ser realizada, e como podemos criar classificações de dados conforme o uso e finalidade do dado. Estudamos o que são backups ou cópias de segurança e a aplicação da classificação de dados para a execução destes processos de backups. Aprendemos também sobre as diversas formas de realizar as cópias de segurança, a frequência com que podem ser feitas e quais as implicações de cada opção. Quanto à utilização de mídias removíveis, falamos sobre os controles que devemos ao utilizá-las e as implicações que o uso desregrado delas pode trazer para a segurança da informação.



Agora é com você!

- 1) Pesquise na sua escola, ou na de algum amigo, se existe classificação de dados e quais são as classificações, detalhando as características de cada uma. Monte uma tabela com as classificações e as características dos dados de cada uma.
- 2) Busque informações sobre como são realizados os processos de backup em sua empresa, ou escola, descreva quais tipos de backups são utilizados e identifique qual é a mídia utilizada para tal finalidade.
- 3) Como utilizar pen drives com segurança?
- 4) Cite três perigos da utilização de pen drives ou DVDs em um ambiente de empresas.
- 5) Procure, na sua escola, como pode ser bloqueado o uso das portas USB para conectar um pen drive, ou utilizar CD/DVDs. Explique a seguir como isto é realizado.

10

Criptografia e Certificação Digital

 Para começar

Agora estudaremos a importância da criptografia no contexto da segurança da informação. Seria plenamente possível a existência de um capítulo específico e extenso para discorrermos somente sobre as técnicas e algoritmos matemáticos de criptografia. No entanto, veremos apenas seus princípios básicos, o que já é extremamente atraente, e entenderemos como ela funciona e o que é a certificação digital e para que ela serve.

10.1 Criptografia

Afinal, o que é criptografia?

A criptografia hoje em dia se ocupa muito menos de sigilo do que uns trinta anos atrás, quando justificava plenamente a etimologia da palavra criptografia, que em grego significa escrita oculta.

kryptós	“escondido”
gráphein	“escrita”

A criptografia é um método de transformar os dados originais, chamados de texto simples ou de texto puro, em algo aparentemente aleatório e ilegível, conhecido por texto cifrado. Ela é um dos principais mecanismos de segurança utilizado na proteção contra os riscos associados ao princípio da confidencialidade.



Figura 10.1 – Dados criptografados.

Uma vez que um texto simples se transforma em texto cifrado, nenhum ser humano, ou máquina, pode processá-lo adequadamente até que seja descriptografado.

Este processo permite que sejam realizadas transmissões de informações confidenciais por meio de canais inseguros, sem riscos de acontecer uma divulgação não autorizada.



O processo de cifragem transforma um texto simples em um texto cifrado e o processo de descriptografia transforma um texto cifrado em um texto simples.

Figura 10.2 – Processo de criptografia.

Em um primeiro momento pode parecer um assunto complicado. Mas não é necessário ser um matemático experiente para entendê-la.

Neste livro, não a estudaremos tão profundamente, apesar de ser um assunto envolvente para quem gosta de desafios. Para aproveitar os benefícios de que codificar, emaranhar dados irá proporciona a você, buscando garantir que seus dados não sejam lidos por qualquer intruso, não é necessário estudá-la tão profundamente, apesar de ser um assunto extremamente envolvente para quem gosta de desafios, e nem ser nenhum matemático experiente.

Um sistema que proporciona criptografia e descriptografia é conhecido como sistema criptográfico e pode ser criado por meio de componentes de hardware ou código de um programa de uma aplicação qualquer.

Hoje, a criptografia está integrada ou pode ser facilmente adicionada à maioria dos sistemas operacionais e aplicativos, e para utilizá-la, na maioria das vezes, basta a algumas configurações ou cliques do mouse.

A informação será transformada em algo ilegível, de forma que possa ser conhecida apenas por pessoa autorizada ou, no caso de mensagem, pelo destinatário efetivo.

A maioria dos métodos de criptografia usa um valor secreto chamado chave (geralmente uma longa sequência de bits) que trabalha com um algoritmo matemático para criptografar e descriptografar o texto.

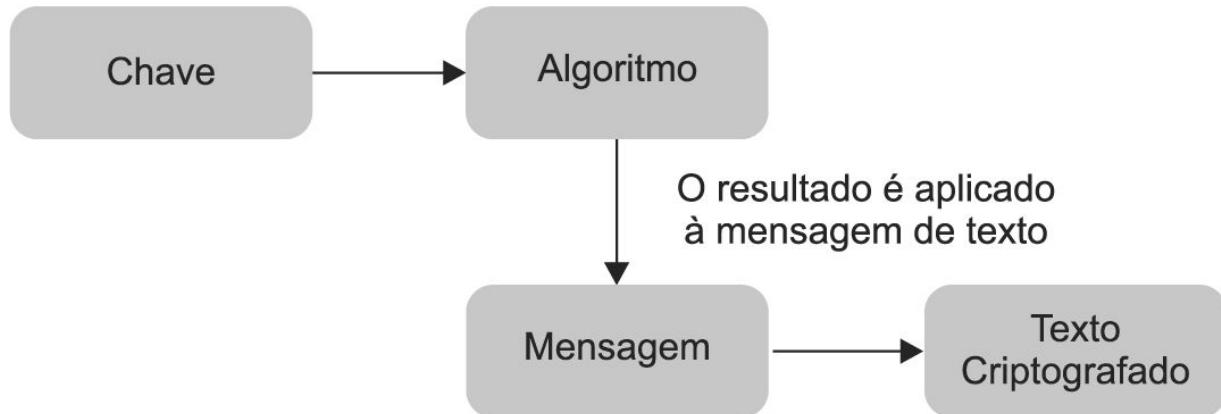


Figura 10.3 – Processo criptográfico com 1.

Algoritmos Criptográficos: são as funções matemáticas utilizadas na codificação dos dados garantindo segredo e autenticação.

Os algoritmos devem ser conhecidos e testados, e a segurança deve basear-se completamente nesta chave secreta, que deve ter tamanho suficiente para não ser descoberta de forma simples por tentativa e erro.

A maneira como o trabalho de criptografia é realizado pode ser mantida em segredo, mas muitos destes métodos são publicamente conhecidos e bem compreendidos.

O segredo do uso de um algoritmo de criptografia bem conhecido é a chave.

Esta chave pode ser qualquer valor composto por uma grande sequência de bits aleatórios.

Você pode neste momento questionar: é apenas um número aleatório de bits amontoados?

Um algoritmo contém um chamado “keyspace”, que é uma gama de valores que podem ser utilizados para a construção de uma chave.

A chave é composta de valores aleatórios nesta gama de valores (keyspace).

Quanto maior o keyspace, mais valores disponíveis podem ser usados para representar chaves diferentes, e mais aleatórias as chaves são, o que torna mais difícil para invasores entendê-las e quebrar a criptografia utilizada.

Para entendermos os tipos de codificação, a Figura 10.4 é uma referência de quem é quem em criptografia:

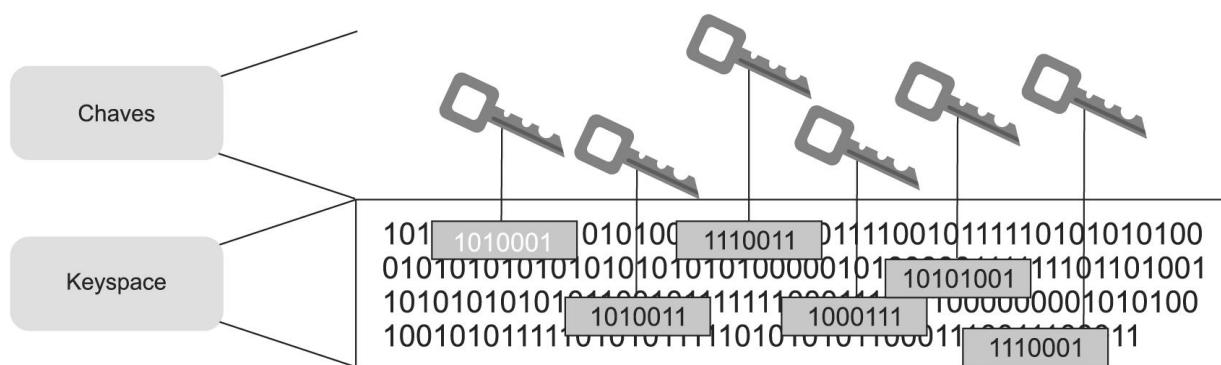


Figura 10.4 – Chaves criptográficas 1.

Devemos ter em mente que uma chave criptográfica é um tipo de segredo para codificar e decodificar uma informação.

Para entendermos a importância da criptografia, podemos observar um exemplo clássico, que são as compras online. Nelas, todos os requisitos para a aplicação do princípio de segurança da informação são claramente necessários neste processo crítico de troca de informações.

A informação que permite a transação – valor e descrição do produto – precisa estar disponível no dia e na hora que o cliente desejar realizá-la (disponibilidade), o valor desta transação não pode ser alterado (integridade) e, o mais importante, somente o cliente que está comprando e o vendedor devem ter acesso a esta transação (confidencialidade e controle de acesso).

O cliente que está comprando deve ser realmente quem diz ser (autenticidade e controle de acesso), além do mais o cliente tem de ter meios de provar o pagamento e o vendedor não pode negar o recebimento (não repúdio). E, por fim, o conhecimento do conteúdo desta transação deve ser restrito aos envolvidos na mesma (privacidade).

Para garantirmos estas condições é necessária a utilização de técnicas de criptografia entre o remetente e o destinatário. Os dados são criptografados, impedindo que outros vejam e entendam os dados que estão sendo trocados entre os dois: o cliente (remetente) e o vendedor (destinatário).

Este processo de codificação existe em dois tipos, dependendo do tipo da chave de criptografia utilizada: simétrica ou assimétrica.

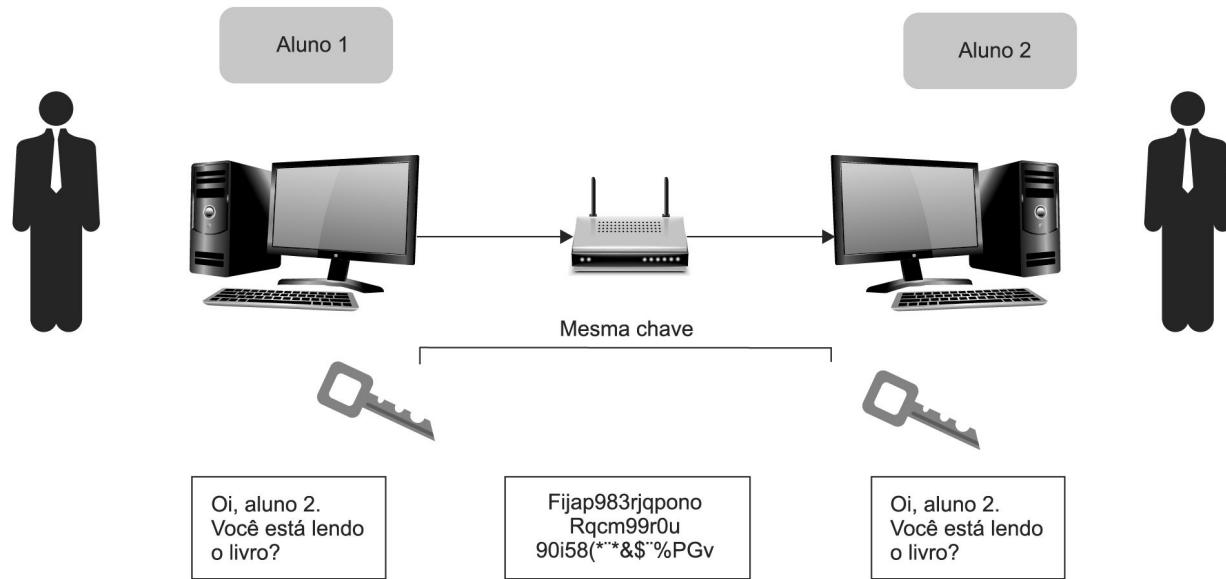


Figura 10.5 – Criptografia simétrica.

Quando esta chave é a mesma para as duas operações, denominamos de criptografia simétrica, e quando as chaves são diferentes, uma para codificar e outra para decodificar a informação, ou vice-versa, denominamos de criptografia assimétrica .

Observe então que temos sempre um par de chaves, uma no emitente e outra no destinatário.

10.1.1 Criptografia simétrica

Na criptografia simétrica temos esta chave que é representada por uma senha, usada tanto pelo remetente para codificar a mensagem em uma das pontas como pelo destinatário para decodificá-la na outra.

Na Figura 10.5 podemos observar que com a mesma chave, a informação do remetente é codificada, e o destinatário decodifica esta informação.

A principal vantagem da utilização de chave simétrica é a facilidade de uso e rapidez na utilização de métodos de criptografia.

Entretanto, quando essas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (manutenção da confidencialidade da chave).

Isso é um fator negativo nas chaves simétricas. Imagine, por exemplo, que entre você e seus amigos teriam de ser criadas inúmeras chaves que seriam passadas a cada amigo, que assim levaria suas mensagens.

No caso de utilização deste sistema de criptografia, quando a chave de codificação é a mesma utilizada para decodificação, esta última pode facilmente ser obtida a partir do conhecimento da primeira.

No método de criptografia simétrica a segurança é completamente dependente da forma como os usuários protegem a chave.

Isso deve nos mostrar sinais vermelhos, se alguma vez dependemos de algumas pessoas para manter um segredo qualquer.

Lembre que não há maneira de provar quem realmente enviou uma mensagem, se duas pessoas estão usando exatamente a mesma chave.

Ambas as chaves precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o meio de criptografia desejado. É importante saber que durante o processo de compartilhamento esta senha pode ser interceptada.

Por este motivo é fundamental utilizar um canal seguro durante o processo de compartilhamento, sendo este independente do destinatário para comunicação sigilosa, uma vez que qualquer um que tenha acesso à senha poderá descobrir o conteúdo confidencial de uma mensagem.

Pontos Fortes da Criptografia Simétrica:

- » É muito mais rápida que sistemas assimétricos;
- » Difícil de quebrar se usarmos chave de grande tamanho.

Fraqueza da Criptografia Simétrica:

- » Exige um mecanismo seguro para chaves de entrega.

A seguir, alguns exemplos de algoritmos de criptografia de chaves simétricas:

- » Data Encryption Standard (DES)
- » Triple DES (3DES)
- » Blowfish
- » IDEA
- » RC4, RC5 e RC6

Fique de olho!

Vale lembrar que somente com a mesma chave utilizada para codificar é que podemos decodificar a informação.

Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA. Pesquise sobre estes métodos.

Se pretendemos enviar para alguém um arquivo codificado utilizando criptografia simétrica, seu receptor deve saber qual algoritmo foi utilizado e ter conhecimento da senha definida por você.

Amplie seus conhecimentos

Para mais detalhes sobre a criptografia assimétrica, pesquise nos endereços a seguir:

<http://csrc.nist.gov/publications/nistpubs/800-7/node208.html>

<http://developer.nestcape.com/docs/manuals/security/pkin/contents.htm>

www1.tepcom.ru/users/ant/Articles/Pkcstane.html

10.1.2 Criptografia assimétrica

Na criptografia assimétrica são utilizadas duas chaves: uma para realizar a codificação da informação e outra para decodificar esta informação.

Este tipo de criptografia, também chamado criptografia de chave pública, é composto por um sistema para codificar e decodificar uma informação com duas chaves distintas, sendo uma pública (chave pública), que pode ser divulgada, e a outra privada, que deve ser mantida em segredo (chave privada).

Em um sistema de chave pública, o par de chaves é composto de uma chave pública e uma chave privada. Muitas vezes, as chaves públicas são listadas em diretórios e/ou bancos de dados de endereços de e-mail para que estejam disponíveis para quem quiser usar essas chaves para criptografar ou descriptografar dados durante a comunicação com uma pessoa em particular.

As chaves públicas e privadas são matematicamente relacionadas, mas não podem ser derivadas uma a partir da outra.

Funciona da seguinte maneira: se codificarmos a mensagem com a chave privada, ela só será decifrada pela chave pública e vice-versa.

Em um algoritmo de criptografia assimétrica, uma mensagem cifrada com a chave pública pode ser decifrada somente pela sua chave privada correspondente.

Vejamos um exemplo simbólico:

O **aluno 1** pode criptografar uma mensagem com uma chave privada e, em seguida, o receptor pode decifrá-lo com a chave pública do **aluno 1**.

Por descriptografar com a chave pública de **aluno 1**, o receptor pode ter certeza de que a mensagem veio realmente do **aluno 1**.

A mensagem só pode ser decifrada com uma chave pública se a mensagem foi criptografada com a chave privada correspondente a ela.

Isto fornece autenticação, porque o **aluno 1** é o único que possui sua chave privada. Quando o receptor quer ter certeza se o **aluno 1** é o único que pode ler a sua resposta, ele vai criptografar a resposta com a sua chave pública.

Só o **aluno 1** será capaz de decifrar a mensagem, porque ele é o único que tem a chave privada necessária para isso.

A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de quem codifica a informação.

Para entendermos melhor o processo, podemos imaginar que a chave pública de alguém é como um cadeado, pode ficar exposta, enquanto a chave privada, que permitirá abrir este cadeado, é

efetivamente uma chave específica (chave privada) para este cadeado.

Na Figura 10.6 ilustramos a utilização das duas chaves, a pública e a privada, em uma mensagem entre dois alunos.

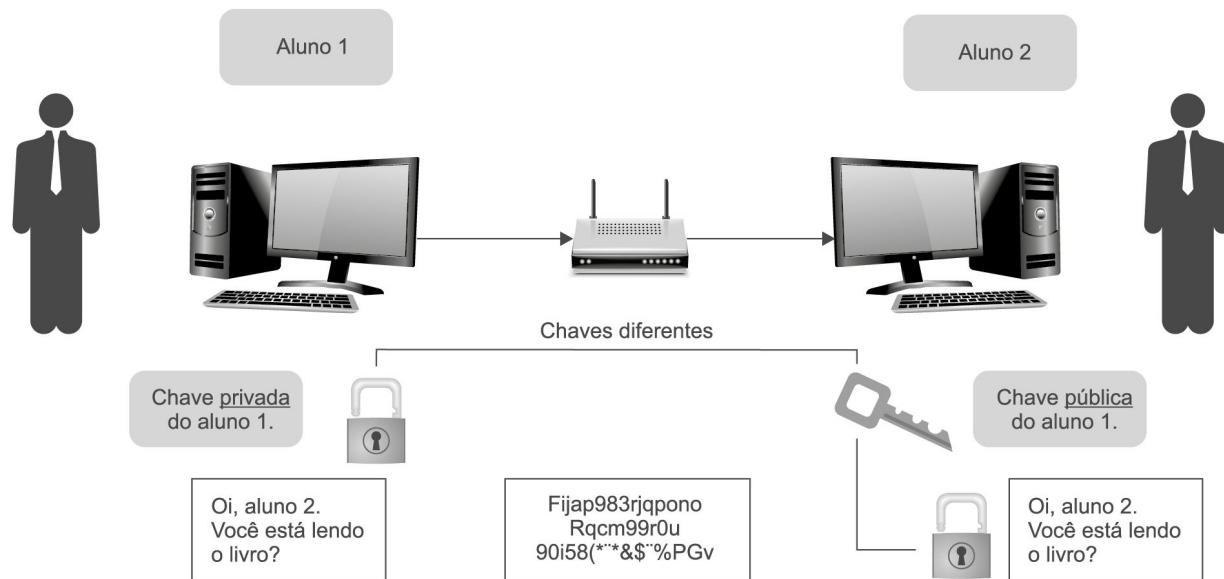


Figura 10.6 – Criptografia assimétrica.

Agora, vamos imaginar que o receptor da mensagem também pode criptografar sua resposta com sua chave privada em vez de usar a chave pública de [aluno 1](#) .

Por que ele faria isso? Ele quer que o [aluno 1](#) saiba que a mensagem veio para ele e não outra pessoa.

Se ele criptografa a resposta com a chave pública de [aluno 1](#) , não fornece autenticidade, porque qualquer pessoa pode obter uma chave pública de [aluno 1](#) .

Se usar sua chave privada para criptografar a mensagem, em seguida, o [aluno 1](#) pode ter certeza de que a mensagem veio dele e de mais ninguém.

As chaves simétricas não oferecem autenticidade desta forma, porque a mesma chave é usada em ambas as extremidades.

Usar uma das chaves secretas não é o suficiente para assegurar que a mensagem foi originada a partir de uma pessoa específica.

Se confidencialidade é o serviço de segurança mais importante para um remetente, ela caracterizaria a necessidade de criptografar o arquivo com a chave pública do destinatário.

Isto é chamado de formato de **mensagem segura**, pois só pode ser decifrada pela pessoa que tem a chave privada correspondente, e fornece uma garantia para o receptor que a única pessoa que poderia ter criptografado a mensagem é o indivíduo que tem a posse dessa chave privada.

Criptografar uma mensagem com a chave privada do remetente é denominado de mensagem aberta porque qualquer um com uma cópia da chave pública correspondente pode descriptografar a mensagem. Desta maneira a confidencialidade não é mais garantida.

Para uma mensagem ter um formato **seguro e assinado**, o remetente deve criptografar a mensagem com sua chave privada e, em seguida, criptografá-la novamente com a chave pública do receptor.

O receptor, então, tem a necessidade de decifrar a mensagem com sua própria chave privada e decifrá-la, outra vez, com a chave pública do remetente.

Para causar confusão a ponto de acharmos que a chave pública é apenas para criptografia e uma chave privada é apenas para descriptografia, destacamos que “cada tipo de chave (pública e privada) pode ser usado para criptografar e descriptografar”.

Enfim:

- » Se os dados são criptografados com uma chave privada, eles não podem ser decifrados com uma chave privada;

- » Se os dados são criptografados com uma chave privada, devem ser decifrados com a chave pública correspondente;
- » Se os dados são criptografados com uma chave pública, devem ser decifrados com a chave privada correspondente.

Observe que a grande vantagem deste tipo de criptografia é permitir que qualquer um envie uma mensagem secreta, apenas utilizando-se da chave pública de quem irá recebê-la.

Como a chave pública está amplamente disponível, não há necessidade obrigatória do envio de chaves como é feito no modelo simétrico.

O algoritmo RSA é a base, atualmente, da maioria das aplicações (softwares) que utilizam criptografia assimétrica. O tamanho desta chave varia entre 512 a 2.048 bits.

Não é possível descobrir o valor de uma chave privada a partir da chave pública (ou vice-versa), ou a partir do próprio texto codificado, o que nos garante a integridade e a autenticidade.

O RSA baseia-se na grande dificuldade dos computadores de realizar a fatoração de números grandes. Assim, as chaves são geradas matematicamente por meio do produto de dois números primos grandes.

Mesmo que se tenha esse produto resultante (que faz parte da chave pública divulgada), a segurança ainda é garantida devido a grande dificuldade de se fatorá-lo e obter os números primos que são essenciais para o algoritmo.

A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido.

Todavia, a criptografia simétrica, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável em virtude de:

- » Ter a necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na internet pode ser bastante complicado); e
- » Existir a dificuldade de gerenciamento de grandes quantidades de chaves (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos, como já salientamos).

A criptografia assimétrica também tem seus aspectos negativos, quais sejam:

- » Infelizmente, o uso do software apenas garante que o dono do par de chaves realizou as operações, e não que o par de chaves em questão pertence realmente a uma pessoa.
- » Não existe nenhum mecanismo que impeça um usuário de gerar um par de chaves com o nome de outro usuário.

Para resolver estes problema, utilizam-se técnicas como certificação digital (algo que seria uma versão digital para a já conhecida “firma reconhecida” dos cartórios).

Amplie seus conhecimentos

Existem outros tipos de criptografia (algoritmos, na verdade) e acreditamos que é ideal você, leitor, pesquisar sobre eles, pois, como comentamos no início do capítulo, este é um assunto muito extenso.

Pesquise mais detalhes sobre Block Cipher e Stream Cipher.

10.2 Certificação digital

Vamos estudar como funciona a certificação digital. Porém, para iniciar este estudo, temos de conhecer os conceitos de hash e assinatura digital.

10.2.1 Função hash

Trata-se de uma função de resumo que é um método criptográfico, que, ao ser aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado hash.⁷

Pode-se utilizar hash para:

- » Verificar a integridade de um arquivo armazenado em um computador, mensagem ou arquivos de backups;
- » Verificar a integridade de um arquivo obtido da internet (alguns sites, além do arquivo em si, também disponibilizam o hash correspondente, para que você possa verificar se o arquivo foi corretamente transmitido e gravado);
- » Gerar assinaturas digitais, como veremos a seguir.

Para verificar a integridade de um arquivo, podemos calcular o hash dele e, quando julgar necessário, gerar novamente este valor.

Se os dois hashes forem iguais, podemos concluir que o arquivo não foi alterado.

Caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado.

10.2.2 Assinatura digital

Uma assinatura digital permite comprovar a autenticidade e a integridade de uma informação, isto é, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, apenas seu dono poderia ter feito isto.

A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

A chave pública pode ser livremente divulgada. Entretanto, se não houver como comprovar a quem ela pertence, podemos acabar nos comunicando, de forma codificada, diretamente com um impostor, ou com alguém que não seja quem diz ser, mas que está se passando por outra pessoa por meio da assinatura digital – da mesma maneira que alguém falsifica uma assinatura no papel, passando-se por outro.

Uma assinatura digital é um valor hash criptografado. A partir do exemplo anterior, se o aluno 1 queria garantir que a mensagem enviada para o aluno 2 não foi modificada e que este último tenha a certeza de que havia sido realmente ele quem enviou a mensagem (aluno 1), ele pode assinar digitalmente a mensagem.

Em outros termos, uma função hash one-way seria executada na mensagem e, em seguida, o aluno 1 esse valor de hash junto com sua chave privada.

Quando o aluno 2 recebe a mensagem, ela vai executar a função de hash na mensagem e obter um valor do hash.

Em seguida, o valor de hash enviado com a chave pública do aluno 1. Ele então compara os dois valores e, se forem iguais, o aluno 2 saberá que a mensagem não foi modificada.

Vamos tentar ser claros sobre todas as opções disponíveis dentro do contexto de criptografia, porque diferentes etapas e algoritmos nos oferecem diferentes tipos de serviços de segurança:

- » Uma mensagem pode ser criptografada, o que fornece confidencialidade;
- » Uma mensagem pode ter um hash, o que fornece integridade;
- » Uma mensagem pode ser assinada digitalmente, o que fornece autenticação e integridade;
- » Uma mensagem pode ser criptografada e assinada digitalmente, o que fornece autenticação, confidencialidade e integridade.

Importante saber que, quando a função de hashing está envolvida, um algoritmo de hash é usado, e não um algoritmo de criptografia.

A assinatura digital é o valor hash criptografado de uma mensagem.

O ato de assinatura, apresentado na Figura 10.7 a seguir, significa criptografar o valor hash da mensagem com a chave privada:

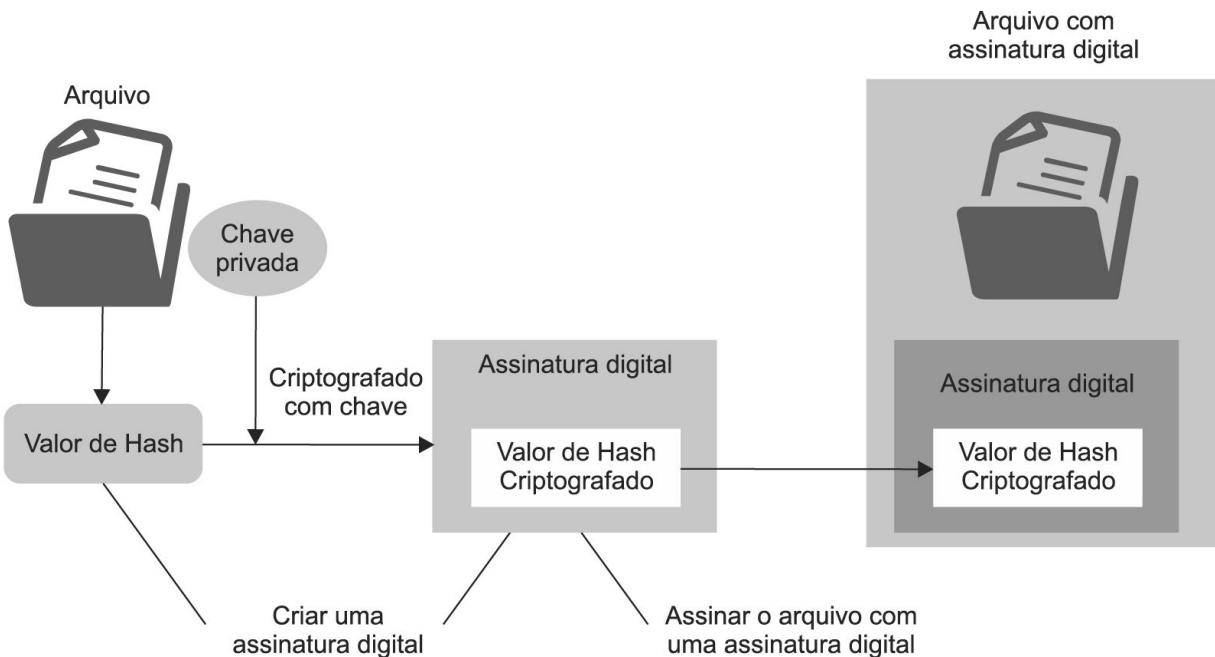


Figura 10.7 – Criação de assinatura digital.

10.2.3 Certificado digital

Com a utilização de criptografia com chave pública, o gerenciamento de chaves passa a ter dois novos aspectos: (1) primeiro, deve-se previamente localizar a chave pública de qualquer pessoa com quem se deseja comunicar; e (2) em seguida, deve-se obter uma garantia de que a chave pública encontrada seja realmente proveniente daquela pessoa.

Sem esta garantia, um intruso, alguém mal-intencionado, pode convencer os interlocutores de que chaves públicas falsas pertencem a eles.

Estabelecendo um processo de confiança entre os interlocutores, este mal-intencionado pode passar como se fosse ambos.

Deste modo, quando um emissor enviar uma mensagem ao receptor solicitando sua chave pública, o mal-intencionado poderá interceptá-la e devolver-lhe uma chave pública forjada por ele.

Ele poderá também fazer o mesmo com o receptor. Desta forma, cada um dos lados pensará que está se comunicando com o outro, quando na verdade estão sendo interceptados por alguém, que pode decifrar todas as mensagens, criptografá-las novamente ou, se preferir, até substituí-las por outras mensagens.

Com este ataque, um interceptador pode causar ainda mais danos do que causaria se conseguisse quebrar e descobrir o algoritmo de criptografia utilizado pelos dois usuários das mensagens.

A garantia para evitar este tipo de ataque e interceptação é realizada pelos certificados de chave pública, chamados **certificado digital**, que consistem em chaves públicas garantidas por uma organização certificadora de confiança.

O **certificado digital** é um documento eletrônico que contém dados sobre a pessoa ou entidade que o utiliza para comprovação mútua de autenticidade.

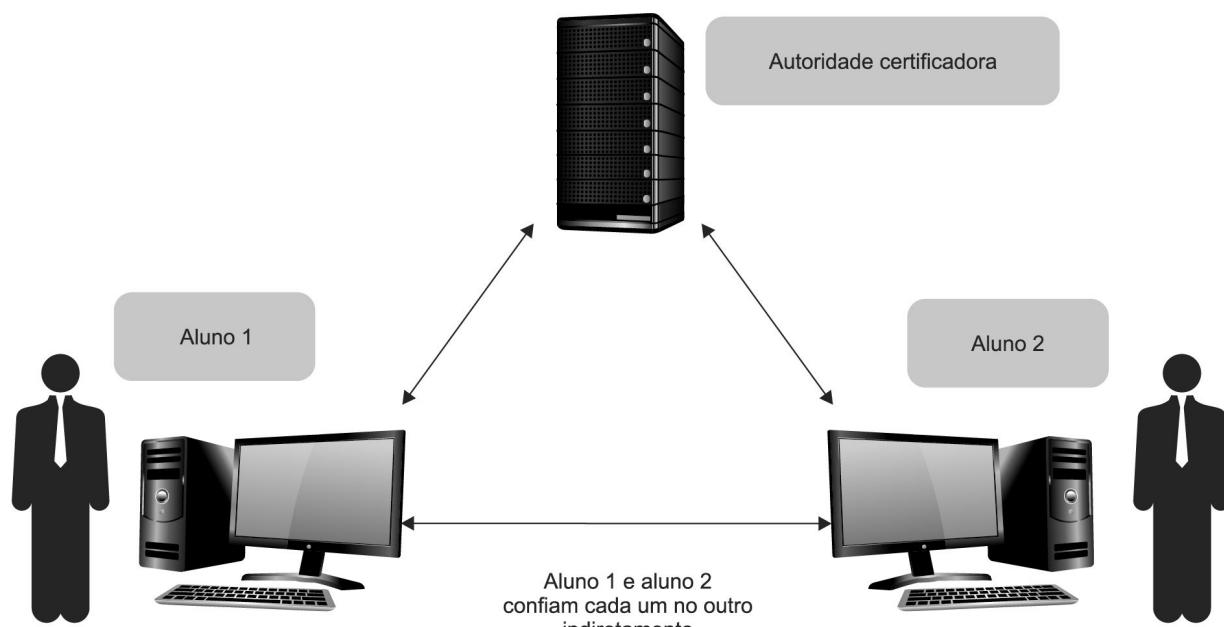


Figura 10.8 – Utilização de certificação digital.

Com a função parecida a de um RG, ou CPF, ele é uma carteira de identidade eletrônica, permitindo que uma transação realizada via internet torne-se perfeitamente segura, já que as partes envolvidas deverão apresentar mutuamente suas credenciais, comprovando suas identidades.

Com a certificação digital, um usuário tem a opção de utilizar sua assinatura digital, garantindo, numa troca de documentos, autenticação, sigilo e integridade de conteúdo.

Assim, os documentos que trafegam eletronicamente, para possuírem reconhecimento legal, não mais precisam ser convertidos em papel e assinados.

Por exemplo, no caso de um passaporte, a entidade responsável pela emissão e pela veracidade dos dados é a Polícia Federal.

No caso do certificado digital esta entidade é chamada de autoridade certificadora (AC).

Uma autoridade certificadora emissora é também responsável por publicar informações sobre certificados que não são mais confiáveis.

Sempre que a AC descobre ou é informada que um certificado não é mais confiável, ela o inclui em uma “lista negra”, chamada “Lista de Certificados Revogados” (LCR), para que os usuários possam ser informados. A LCR é um arquivo eletrônico publicado periodicamente pela autoridade certificadora, contendo o número de série dos certificados que não são mais válidos e a data de revogação.

Quando uma pessoa faz um pedido de certificado digital, a AC verifica os dados de identidade da pessoa, constrói o certificado, os dados do certificado dela e entrega-o para o solicitante.

Quando outra pessoa quer se comunicar com essa pessoa, o AC basicamente atesta e garante a identidade dessa pessoa.

Neste caso, a criptografia com chaves públicas é baseada na confiança dos usuários na autoridade certificadora.

Um certificado digital pode ser utilizado para finalidades específicas. Assim sendo existem, por exemplo, certificados digitais específicos para emissão de notas fiscais eletrônicas, para relacionamento com a Receita Federal, para órgãos públicos em geral, ou simplesmente para proteger um servidor de internet (servidor web).

Em caso de pessoa física, a emissão de uma certificação digital exige o comparecimento na autoridade certificadora, não sendo permitida a utilização de uma procuração para obter um certificado digital.

A **validação presencial** é o momento da confirmação da identidade do titular solicitante do certificado digital, seja este para pessoa física ou jurídica. Ou seja, é quando se comprova a veracidade dos dados informados no momento em que foi realizada a solicitação do certificado digital por meio da presença do titular e a apresentação de documentos obrigatórios

No caso de empresas a procuração é aceita somente para a representação do responsável pelo certificado digital, desde que o ato constitutivo da empresa não vede tal ação.

As procurações devem ser públicas, lavradas em cartório e específicas para atuar perante ICP Brasil (*Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira*).

Conforme resolução nº 79 do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP – Brasil), publicada no *Diário Oficial da União* em 7 de junho de 2010, para “comprovar que a pessoa física que se apresenta como responsável pelo uso do

certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, é admitida a procuração somente para a representação do titular do Certificado Digital, ou seja, o(s) representante(s) legal (is) da Pessoa Jurídica solicitante, apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante ICP – Brasil" (item 3.1.1.1, alínea "a", item i do DOC-ICP-05, versão 3.4). Fonte: <http://www.certisign.com.br>

Importante: No caso de Certificados e-CNPJ, o representante legal da empresa perante a Receita Federal do Brasil não poderá ser representado por procuração.

Todos estes aspectos visam dar a garantia da identidade de quem (pessoa física ou pessoa jurídica) possuirá uma certificação digital.

Podemos verificar em um navegador as informações dos certificados que determinado computador contém.

Em ferramentas, selecione “opções” e vá para a aba de conteúdo. Será, então, apresentada uma lista dos certificados. Ao clicar em um específico, poderemos ver os detalhes dele, como na Figura 10.9:

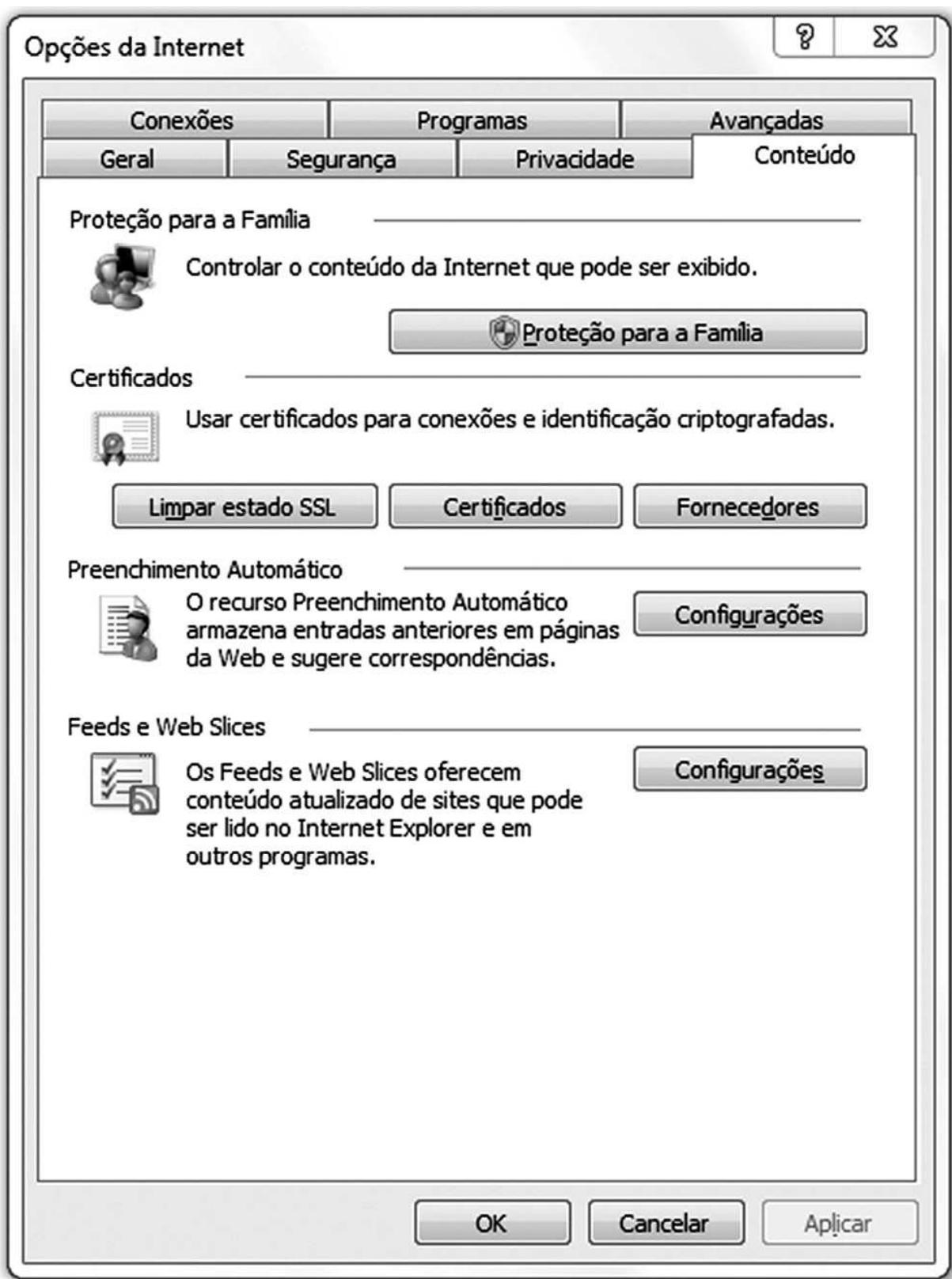


Figura 10.9 – Verificando certificados no browser.

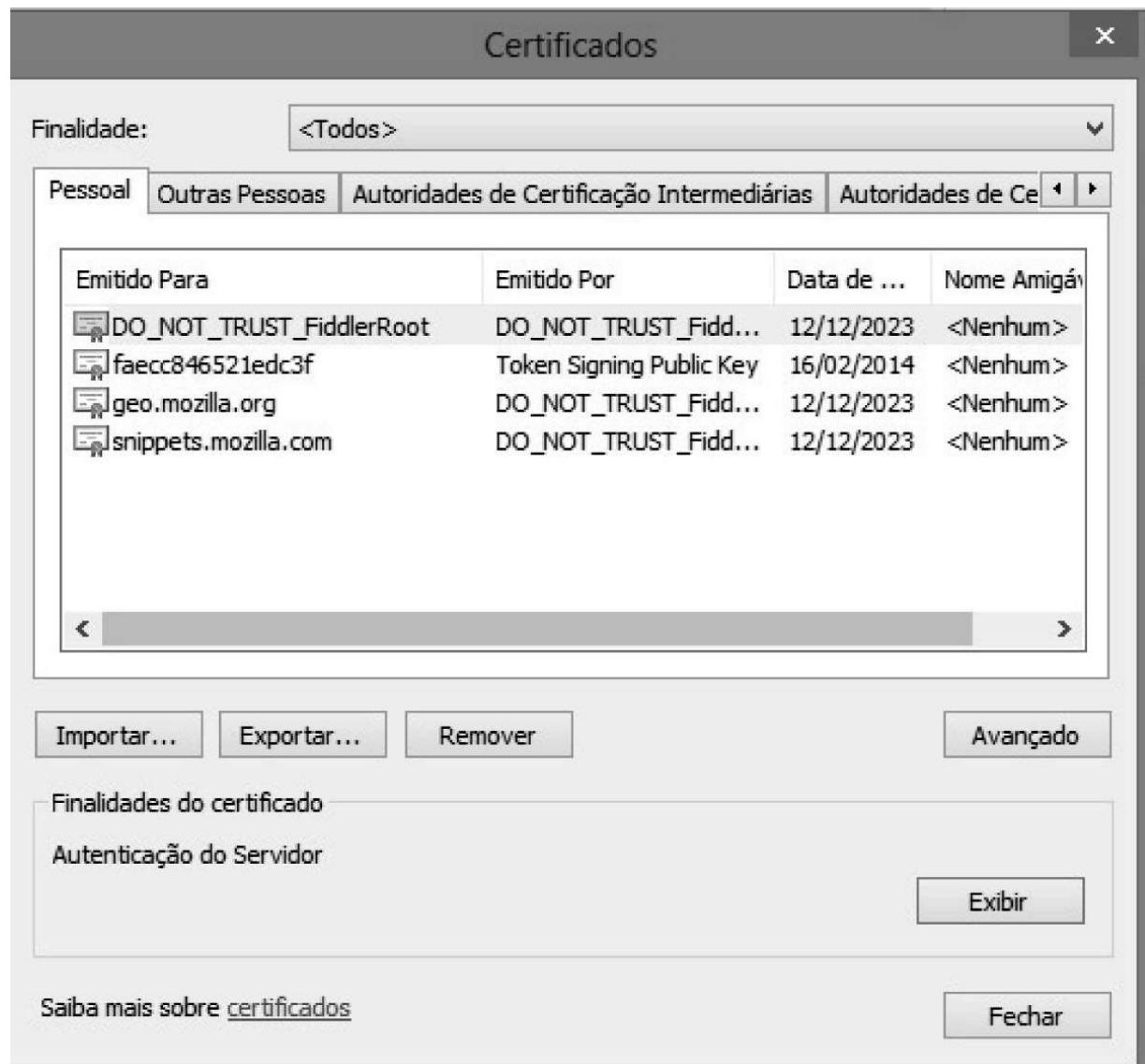


Figura 10.10 – Lista de certificados no browser.



Figura 10.11 – Detalhes do certificado.

Poderemos selecionar um dos certificados e exibir sua situação. Veremos, assim, se este certificado está correto ou se tem algum problema.

No Brasil, o órgão da autoridade certificadora raiz é o ICP-Brasil (AC-Raiz), ele é o executor das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

São autoridades certificadoras no país: Serpro (AC-SERPRO), Caixa Econômica Federal (AC-CAIXA), Serasa Experian (AC-SERASA), Receita Federal do Brasil, (AC-RFB), Certisign (AC-Certisign), Imprensa Oficial do Estado de São Paulo (AC-IOSP), Autoridade Certificadora da Justiça (AC-JUS), Autoridade Certificadora da Presidência da República (AC-PR) e Casa da Moeda do Brasil (AC-CMB).

A Autoridade Certificadora Raiz tem autoridade de emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu, sendo também encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil.

Além disso, a Autoridade Certificadora Raiz verifica se as autoridades certificadoras (ACs) estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

10.2.4 Política de e-mail

Dentre os controles de segurança da informação em uma empresa, destaca-se a elaboração de normas para a utilização de programas de e-mail, ou seja, a utilização de e-mail da empresa e particulares no ambiente controlado de trabalho.

É normal que as empresas limitem a utilização de contas de e-mail particulares, como o “Gmail”, nas instalações da empresa. Isto é compreensível apesar de que aparentemente representa um cerceamento da liberdade do indivíduo.



deboy/Shutterstock.com

Figura 10.12 – Políticas de e-mail.

O objetivo principal deste tipo de restrição é eliminar a sobrecarga das comunicações da empresa com envio e recebimento de e-mails particulares.

Dentro dos procedimentos e normas constantes da política de segurança da informação deve existir sempre recomendações para controles do uso de e-mail profissional da empresa como:

- » Não reenvie e-mails do tipo corrente, aviso de vírus, avisos de empresas de aviação, provedores de internet, companhias telefônicas, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa etc.;
- » Limitar o envio de e-mails para no máximo dez pessoas por vez (to, cc). Comunicações para grande número de funcionários deve ser atributo da área de comunicação corporativa e nunca de todos os funcionários;
- » Não utilize e-mails com cópia oculta (bcc);

- » Evite anexos muito grandes, normalmente a área de segurança de TI limita o tamanho máximo das mensagens em torno de 1 Gb;
- » Não abra os e-mails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis e famosos dos últimos tempos tinham assuntos como: I LOVE YOU, Branca de Neve pornô etc.
- » O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los. Se for solicitada a interrupção do envio, esta deve ser acatada e o envio não deverá mais acontecer. Neste ponto é importante observar se a pessoa para quem se deseja enviar o e-mail é realmente a selecionada no catálogo de endereços do programa de e-mail, procurando ao máximo evitar o envio de e-mails desnecessários para pessoas que não devem ser envolvidas com o assunto;
- » Deve ser obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e anexos inúteis;
- » Deve ser sempre obrigatório a utilização do software homologado pela área de TI para ser o cliente de e-mail;
- » Para garantir a perfeita distribuição dos e-mails profissionais, convém utilizar os controles de solicitação de confirmação de recebimento da mensagem, permitindo assim que exista controle de que a mensagem foi recebida pelo destinatário. Logo devem ser solicitadas notificações no mínimo de “recebimento” e “leitura”;
- » Ter como norma não abrir anexos com as extensões .bat, .exe, .src, .lnk e .com, se não tiver certeza absoluta de que solicitou esse e-mail;
- » Não devem ser enviadas mensagens de e-mail cujo conteúdo seja confidencial em nenhuma hipótese para endereços que sejam fora do domínio de e-mail da empresa;

- » Criar padrões de assinatura fixa de e-mail para os funcionários, buscando assim que todos os e-mails enviados tenham clara a identificação do remetente.

Importante é entender que o e-mail corporativo é o serviço de correio eletrônico disponibilizado pela empresa ao empregado, com a finalidade única e exclusiva de que este mantenha contato com os clientes e demais membros da empresa por meio do canal apropriado.

Tecnicamente não há diferenças entre um e-mail corporativo e pessoal. No entanto, devido à complexidade de relacionamento existente e mesmo a responsabilidade que a empresa possui perante seus clientes pelas atitudes de seus empregados, há que se ter um tratamento diferenciado com o serviço de correio eletrônico empresarial.

Além da existência da responsabilidade objetiva da empresa frente às comunicações realizadas em seu nome por seus funcionários, também existe a questão da imagem que esta transmite aos seus clientes. Um e-mail utilizado de forma incorreta ou mesmo contendo grosserias pode arranhar a reputação de uma empresa, determinando o fracasso de um grande investimento para a construção de sua imagem. Isto é o que chamamos de ética de comunicação por e-mail corporativo.

10.2.4.1 Aspectos legais

Chamamos atenção para o fato de que e-mails enviados que causem algum dano à empresa, pessoas da empresa, ou a clientes e fornecedores, podem ferir o Código Civil. O artigo 186 tem como redação:

Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

E o artigo 927 do mesmo Código Civil tem como redação:

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Assim como as demais ferramentas de trabalho, o e-mail corporativo deve ter uso restrito para assuntos profissionais.

A má utilização do e-mail corporativo pode ser causa de demissão.

10.2.4.2 Aspectos éticos de e-mail

Quando finalizar uma mensagem, a forma de cumprimento “Atenciosamente”, ou “Att”, é a mais indicada pela ética de e-mails.

Quando há um pouco mais de informalidade entre colegas, o “abraço” ou “abs” pode ser utilizado, mas nunca utilize em e-mails corporativos a finalização com “beijos” ou “bjs”, mesmo que seja para destinatários do sexo feminino. Este tipo de finalização deve estar restrito ao seu círculo de relacionamento pessoal.

Utilize sempre um corretor ortográfico e gramatical do programa cliente de e-mail ao redigir o texto da mensagem, ou tenha um dicionário por perto. Não arrisque sua credibilidade por conta de uma cedilha ou letra trocada.

Como em qualquer outro texto, a capacidade de escrita de uma pessoa está constantemente sendo analisada nos e-mails, por isso a necessidade de sempre respeitar as regras gramaticais e o uso de vírgulas.

O uso do português informal ou cotidiano não é recomendado por ética, em mensagens relacionadas à rotina de trabalho.

Muito importante lembrarmos que gírias, palavrões ou palavras agressivas são completamente proibidos em e-mails profissionais.



Erdal Bayhan/Shutterstock.com

Figura 10.13 – Ética em e-mails.

E lembre-se sempre: não encha a caixa postal de seus colegas com mensagens de piadas e fotos, mesmo que seu objetivo seja mero entretenimento e descontração geral.

Vamos recapitular?

Neste capítulo estudamos o que é criptografia e qual é sua utilização para manter a confidencialidade na troca de mensagens entre usuários. Falamos também sobre os principais métodos deste processo de codificação de textos, como eles funcionam durante o processo de troca de informações.

Aprendemos quais são os métodos de criptografia, as vantagens e desvantagens de cada um deles (criptografia simétrica e assimétrica) e como são criadas as chaves privadas e públicas.

Estudamos, ainda, os conceitos de assinatura digital, o que significa uma certificação digital, o que é uma assinatura digital, como este processo funciona nas comunicações entre computadores e, por fim, como se relacionam as entidades certificadoras com o processo de troca de mensagens para dar-nos garantia de integridade, confidencialidade e autenticidade.



Agora é com você!

- 1) Criptografia simétrica é um método de codificação que utiliza.
- 2) A criptografia assimétrica é utilizada em certificação digital? Pesquise e explique.
- 3) O que caracterizaria que uma mensagem foi modificada?
- 4) Descreva em uma frase o que é uma assinatura digital.
- 5) Qual é autoridade certificadora de sua escola? Existe certificado digital para a escola acessar órgãos públicos federais?
- 6) A assinatura digital busca resolver dois problemas não garantidos apenas com uso da criptografia para codificar as informações.

⁷ O hash é gerado de tal forma que não é possível realizar o processamento inverso para se obter a informação original. Além disso, qualquer alteração na informação original produzirá um hash distinto. Apesar de ser teoricamente possível que informações diferentes gerem hashes iguais, a probabilidade disto ocorrer é significativamente baixa.

11

Segurança Física

 **Para começar**

Este capítulo apresentará os aspectos físicos da segurança da informação, onde esta segurança é afetada e como minimizar e prevenir que problemas físicos com equipamentos provoquem quebra dos princípios de integridade, confidencialidade e disponibilidade. Fazem parte deste contexto inclusive acidentes naturais como chuvas, enchentes e incêndios.

11.1 Introdução

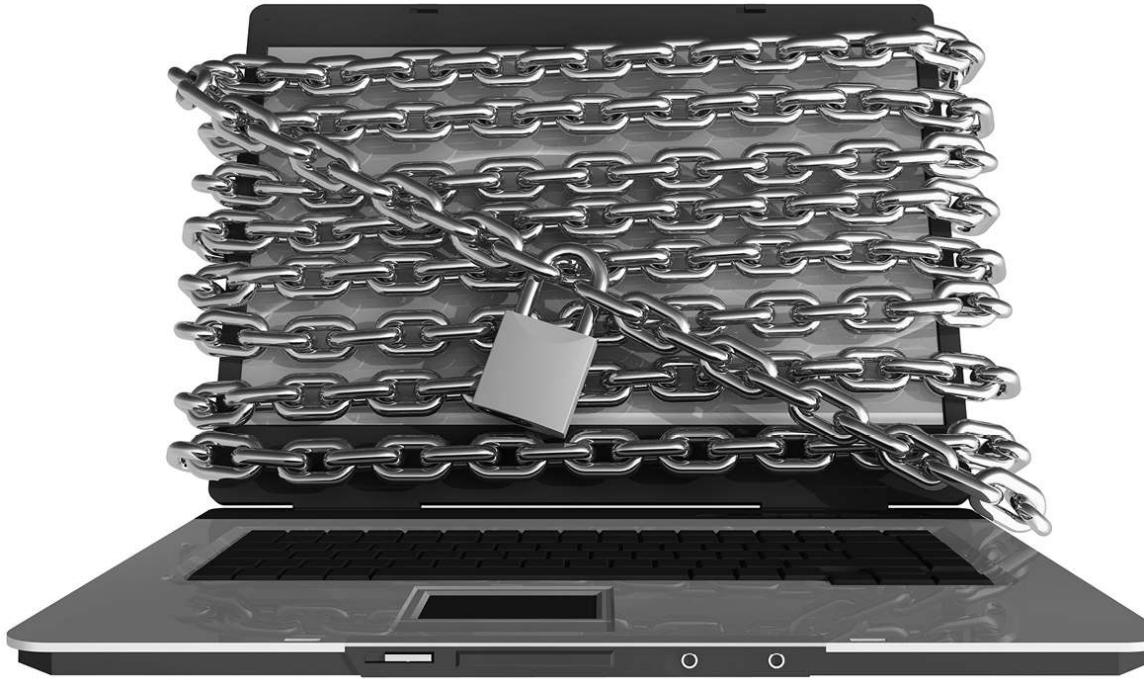
Mas o que é segurança física da informação?

É na realidade a segurança de tudo que não é lógico ou virtual.

Sem a segurança física, o simples acesso de uma pessoa não autorizada a um computador pode resultar em divulgação da informação, alteração da informação e também destruição desta informação.

O principal risco que os componentes físicos da informação estão exposto são roubo, interrupções de serviços por algum dano físico e divulgação não autorizada de informação, ficando a integridade do sistema comprometida.

Furto físico geralmente resulta em computador ou outros dispositivos roubados. A perda real é determinada pelo custo de substituir os artigos furtados mais o custo para restaurar os dados perdidos.



Collina/Shutterstock.com

Figura 11.1 – Proteção contra furto.

Muitas vezes as empresas só realizam um inventário de seu hardware e fornecem estimativas de valor que estão ligados à análise de risco. Assim, elas determinam qual seria o custo para a empresa caso o equipamento fosse roubado ou destruído.

No entanto, as informações contidas dentro do equipamento podem ser muito mais valiosas do que o próprio equipamento, e os mecanismos e procedimentos de recuperação adequados também precisam ser considerados na avaliação dos riscos, para que esta seja uma avaliação mais realista e correta.

A interrupção dos serviços pode ser a perda de serviços de informática em si, perda dos recursos de energia, de abastecimento de água, de controle de temperatura e hoje, principalmente, a perda mesmo que momentânea dos serviços de telecomunicações.

Se uma empresa perde o fornecimento de energia, ela também pode perder seus sistemas elétricos de segurança e sistemas de detecção de intrusão computadorizados.

O grau de dependência de uma empresa dos serviços de telecomunicações determinará se as opções de backup serão postas em prática para garantir a redundância de circuitos ou de comunicação que possam ser ativadas de acordo com a necessidade.

11.2 Segurança do ambiente

No tocante ao ambiente de trabalho de uma empresa, os seguintes elementos devem ser checados continuamente: mesas e armários trancados, estações de trabalho protegidas contra acessos indevidos e furto, disposição e proteção das mídias magnéticas de armazenamento (lembre que falamos dos cofres para as mídias de backup), cabeamento de rede padronizado e seguro, informações protegidas (em meio magnético e papel), documentos sobre as mesas, descarte de informações (se existem trituradoras de papéis), áreas de circulação de visitantes, áreas restritas etc.

A identificação das pessoas que circulam em uma empresa não pode ser tratada sem um rígido controle de identificação de visitantes, terceiros e dos próprios funcionários.

O acesso deve possuir áreas restritas na áreas de desenvolvimento de sistemas e operações, assim como a área do data center deve ser altamente restrita, inclusive aos funcionários da empresa, excetuando-se os profissionais da TI responsáveis pelo monitoramento dos recursos tecnológicos ali existentes.

Hoje, nas empresas, não é mais suficiente a existência de equipamentos como nobreaks. A exceção são as estações de trabalho, ou para garantir o funcionamento dos servidores e equipamentos de armazenamento (storage) e comunicação básicos de rede, tais como roteadores, controladoras etc., sendo devido ao tamanho e importância da informação, que se atua com geradores de energia, que entram em operação imediatamente após uma queda da energia fornecida externamente.

A funcionalidade dos equipamentos nobreak deve ser sempre considerada, pois eles mantêm ininterrupto o fornecimento de energia mínima necessária no instante da interrupção. Porém, como são compostos por baterias que fornecem esta energia, dependendo do tamanho da instalação, esta garantia de funcionamento não é muito superior a cinco minutos.

O custo de parada de sistemas e disponibilidade de informações é relativo aos negócios que param de ser executados durante a interrupção, como faturamento, vendas, produção etc.

Temos de considerar outros fatores do ambiente e estabelecer controles para a proteção e segurança física do ambiente e do data center (antigamente chamado de CPD):

- » Ter controle de acesso de entrada física nos ambientes seguros e no data center;
- » Ter geradores de energia e nobreaks que garantam a continuidade de negócios da empresa;
- » Ter monitoramento de câmeras CFTV (circuito fechado de TV) nos ambientes seguros e no data center;
- » Ter uma rede de supressão de fogo a gás no data center;
- » Ter meios e equipamentos de detecção e extinção de incêndio no ambiente do data center.



Figura 11.2 – Data center.

Atualmente, com o advento da computação móvel, a utilização de notebooks e tablets no ambiente de trabalho é intensa, e com isso a segurança interna da empresa deve ser considerada, pois os casos de furto de equipamentos móveis têm crescido assustadoramente.

O travamento dos notebooks e tablets na mesa de trabalho é um controle relativamente eficaz para que se evite furtos, já que esconder um notebook é um trabalho bem simples para quem deseja executar um furto deste tipo.

Sistemas de supressão de incêndio à base de água (por exemplo, sprinklers) são projetados para proteger pessoas e estruturas. Mas, quando se trata de proteger maquinário de alto valor, computadores e outros aparelhos eletrônicos, a água pode ser mais prejudicial do que o próprio fogo.

No momento tecnológico atual, a utilização de sistemas de supressão a gás é o mais indicado, pois além de não serem mais tóxicos, como antigamente (usavam gás Halon 1301), proporcionam uma rápida extinção de incêndios sem afetar os equipamentos de um data center, e ainda possibilitam que o processo de extinção aconteça com pessoas no ambiente em risco.



Jamesbin/Shutterstock.com

Figura 11.3 – Supressão de fogo a gás.

Por incrível que pareça, a proteção contra desastres naturais como chuvas, enchentes e descargas elétricas também deve ser considerada nos controles de proteção do ambiente do data center.

É muito comum em temporais ocorrerem infiltrações de água nos ambientes do data center de uma empresa, mesmo com todos os cuidados de construção. Logo existe a necessidade de integração entre equipes de segurança de TI e equipes de manutenção predial constante.

As máquinas sensíveis, tais como conjuntos de servidores, devem estar instaladas em compartimentos de acesso restrito. Em geral, estes sistemas possuem um posto de trabalho especial, normalmente designado por “console”, que fornece ao respectivo utilizador alguns direitos adicionais. Dependendo do sistema, podem ser:

- » visualização de mensagens do sistema;

- » intervenção durante o “boot” (fácil de provocar por quem tem acesso físico);
- » único posto onde se permite a “entrada” do administrador;
- » acesso livre a todo o sistema operacional de rede.

Lembrando sempre que as estações de trabalho dentro da empresa são geralmente mais acessíveis fisicamente que o ambiente físico, onde estão servidores e equipamentos de armazenamento e comunicação centralizados.

Normalmente as estações de trabalho possuem discos locais e os usuários devem ser estimulados a manter os seus trabalhos e informações nos servidores da rede.

Além de evitarem a possibilidade de acesso local, beneficiam-se de backups periódicos. É claro que existe o fator de aumento de tráfego de dados nas linhas de comunicação, entretanto os ganhos com a integridade e disponibilidade da informação são sensíveis.

Fique de olho!

Não instalar em áreas de acesso público equipamentos que permitam o acesso à rede interna da corporação.

Uma lista das ameaças de segurança física poderia conter os seguintes itens:

- » Incêndio (fogo e fumaça);
- » Água (vazamentos, corrosão, enchentes);
- » Tremores e abalos sísmicos;
- » Tempestades e furacões;
- » Terrorismo;
- » Sabotagem e vandalismo;
- » Explosões;
- » Roubos, furtos;
- » Desmoronamento de construções;
- » Materiais tóxicos;

- » Interrupção de energia (bombas de pressão, ar-condicionado, elevadores);
- » Interrupção de comunicação (links, voz, dados);
- » Falhas em equipamentos.

Deve ser sempre realizada uma análise para apontar o grau do risco a que a empresa está exposta em decorrência das possíveis ameaças à segurança física.

Considerando sempre quais são as áreas de maior risco (aqueles que podem causar prejuízos ao negócio se um evento motivado por falha na segurança física acontecer), e então serem dirigidos investimentos em procedimentos para que estes riscos sejam minimizados.

A seção 9 da ABNT ISO/IEC 27002:2005 trata da segurança física e do ambiente e define um código de prática para a gestão de segurança da informação, onde são descritos objetivos de controle e controles para evitar acesso físico não autorizado, danos e interferências às instalações e informações da organização.

Convenciona, também, que as instalações de processamento da informação críticas ou sensíveis sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos com barreiras de segurança e controles de acesso apropriados, bem como que sejam fisicamente protegidas contra o acesso não autorizado, danos e interferências (ABNT, 2005, p. 32).



[Blend Images/Shutterstock.com](#)

Figura 11.4 – Segurança de acesso.

Campos (2007, p. 168-9) também argumenta que é importante definir perímetros de segurança para dificultar progressivamente o acesso a determinado ativo de informação. Ou seja, determinar áreas fisicamente isoladas cujo acesso é controlado por meio de barreiras ou controles de entrada física.

Esses controles têm por finalidade garantir que somente pessoas previamente autorizadas possam acessar determinados perímetros de segurança onde são processadas informações críticas para o negócio.

Essas áreas devem ser de difícil acesso ao público, o que justifica a definição do perímetro de segurança.

Amplie seus conhecimentos

Pesquise sobre a norma ABNT ISO/IEC 27002:2005, que trata da segurança da informação, e sobre os pontos da norma que tratam da segurança física.

Uma cópia pode ser encontrada, mesmo que não autorizada pela ABNT, em:

<http://portal.cjf.jus.br/sigjus/arquivos-diversos/NBR-ISO-IEC-17799-2005.PDF/view>



Vamos recapitular?

Neste capítulo você sobre a importância dos controles de acessos de pessoas ao ambiente de TI e as implicações que a ausência deste controle pode causar. Aprendeu também sobre como garantir a integridade física dos equipamentos de rede, e armazenagem de dados contra eventos naturais como catástrofes, quedas de energia, e acidentes físicos intencionais ou acidentais. Como evitar que furtos possam causar prejuízos com a exposição de dados confidenciais, afetando o princípio da confidencialidade.



Agora é com você!

1) Pesquise, junto à segurança da escola, como é realizado o controle das pessoas nas salas que possuem computadores.

Os alunos devem informar com detalhes como é realizado o acesso às salas de laboratório, se é possível acessarem outras instalações de TI. Se existem crachás de identificação para acesso nas áreas de TI.

2) Para testar a segurança de acesso à sala dos servidores da sua escola, ou de sua empresa, descubra a sua localização e teste se você pode entrar desacompanhado nesta sala. Descreva se existe algum processo de identificação de quem entra nesta sala, e como ele é realizado.

Faça uma descrição simples que pode indicar exigência ou

não de identificação das pessoas. Liste se existem notebooks sobre mesas na área administrativa e se é exigida alguma autorização para entrada (descrever) e se seguranças pessoais identificam o acesso nestas áreas.

- 3) Procure saber se existem nobreaks nos servidores da escola e se os computadores da secretaria possuem nobreaks individuais ou coletivos. Descreva o cenário em que se encontram.

Descreva quais equipamentos existem na prática nas áreas que utilizam computadores. Questione e apresente resultados sobre o que acontece em caso de falta de energia.

- 4) Solicite ao seu professor ou na sua empresa sobre como e com que frequência são realizados backups dos dados corporativos de alunos e cursos. Descreva os processos que são utilizados.

Descreva como estes processos são realizados e se existe local apropriado para armazenamento das mídias de cópias.

- 5) Realize uma análise dos riscos físicos existentes nas instalações de sua escola ou de sua empresa e apresente os mesmos em sala de aula para discussão sobre quais seriam as soluções e procedimentos corretos que você entende como faltantes.

Faça um relatório elencando quais riscos o aluno encontrou, e como a escola ou a empresa trata riscos com medidas de segurança. Não basta somente listar os riscos. Deve-se mostrar para cada um elencado como é tratado ou como deveria ser tratado.

6) As instalações dos servidores de sua escola ou empresa possuem algum sistema de controle de incêndios? O aluno deverá descrever o sistema existente, mesmo que sejam somente extintores, descrever os tipos e quantidades. Caso exista algum sistema de combate a fogo automático, apresentar uma descrição dele.

Bibliografia

ADRENALINE. **Novo golpe envolvendo o WhatsApp para desktop é identificado.** Disponível em: <<http://adrenaline.uol.com.br/securanca/noticias.html?bc=45>>. Acesso em: 4 mar. 2014.

ALECRIM, Emerson. **Portas TCP e UDP.** Disponível em: <<http://www.infowester.com/> portastcpudp.php>.

ARBAUGH, W., Wan, Y. e Shankar, N. **Your 802.11 Wireless Network has No Clothes.** Disponível em: <<http://www.cs.umd.edu/%7Ewaa/wireless.pdf>>. Acesso em: fev. 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27002: **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação.** Rio de Janeiro: ABNT, 2005, p. 6-7/32-9.

BATISTI, Julio. **Tutorial de TCP/IP.** Disponível em: <http://www.juliobattisti.com.br/artigos/windows/tcpip_p11.asp>

CAMPOS, André. **Sistema de segurança da informação: controlando os riscos.** 2. ed. Florianópolis: Visual Books, 2007, p. 43-90/167-73.

CARTILHA DE SEGURANÇA NA INTERNET – **CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Disponível em: <<http://cartilha.cert.br/> criptografia/#>. Acesso em: fev-mar. 2014.

CARVALHO, Julio. **A segurança dos Tablets.** Disponível em: <<http://www.profissionaisti.com.br/>> 2011/09/a-seguranca-dos-tablets> - 15 de setembro de 2011. Acesso em: fev. 2014.

CERT. **Segurança em dispositivos móveis.** Disponível em: <<http://cartilha.cert.br/dispositivos-moveis/#>>. Acesso em: 27 mar. 2014.

COSTA, Celso José da e FIGUEIREDO, Luiz Manoel Silva de. **Criptografia geral.** 2. ed. Rio de Janeiro: UFF, 2006, 192p. (Curso de Criptografia e Segurança em Redes).

FARIA, Letícia. **Você sabe o que é um Servidor Firewall?.** Disponível em: <http://www.tudosobreanxere.com.br/index.php/desc_noticias/voce_sabe_o_que_e_um_servidor_firewall>. Acesso em: fev. 2014.

FIGUEIREDO, Luiz Manoel Silva de. **Números primos e criptografia de chave pública.** Rio de Janeiro: UFF, 2006, 180p. (Curso de Criptografia e Segurança em Redes).

HARRIS, Shon. **CISSP All-in-one Certification Exam Guide.** McGraw-Hill/Osborne Media, 2002.

LEWIS, Tobias. **HTTP heuristics for malware detection.** Disponível em: <<http://www.sans.org/reading-room/whitepapers/detection/http-header-heuristics-malware-detection-34460>>. Acesso em: fev 2014.

MISHRA, A. e ARBAUGH, W. **An Initial Security Analysis of the IEEE 802.1X Standard.** Disponível em: <<http://www.cs.umd.edu/~waa/1x.pdf>>. Acesso em: fev. 2014.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec, 2007.

PAULA, Najara Mara Nascimento de. **Segurança da informação com ênfase na segurança física de acervos informacionais.** Natal: UFRN, 2008. 41 f. Monografia (Bacharelado) – Curso de Graduação em Biblioteconomia.

PEIXOTO, Mário C. P. **Engenharia social e segurança da informação na gestão corporativa.** Rio de Janeiro: Brasport, 2006.

REVISTA SEGURANÇA DIGITAL. Disponível em:
<http://segurancadigital.info/atualizacoes-do-site/462-criptografia-simetrica-e-assimetrica>. Acesso em: fev 2014.

SANTOS PINHEIRO, José Mauricio. **Programas de Segurança para Redes Corporativas.** Disponível em:
http://www.projetoderedes.com.br/artigos/artigo_programas_de_seguranca_para_redes_corporativas.php. Acesso em: fev. 2014.

Marcas Registradas

Todas os nomes registrados, marcas registradas ou direitos de uso citados neste livro pertencem aos seus respectivos proprietários.