centro universitário
unifacvest

Crimes Cibernéticos

Segurança da informação

Juliane Adelia Soares

OBJETIVOS DE APRENDIZAGEM

- Relacionar princípios de segurança no contexto de pensamento computacional.
- Descrever as principais ameaças à segurança e crimes cibernéticos.
- Listar técnicas e estratégias para gerenciamento de segurança da informação.

Introdução

Com o avanço da tecnologia, capacidades de pensamento computacional se tornam cada dia mais necessárias. O pensamento computacional envolve uma nova forma de pensar a respeito da resolução de problemas, e, no mundo moderno, possuir essa habilidade traz uma série de benefícios. O problema é que a tecnologia também apresenta alguns riscos, como invasão e roubo de dados confidenciais, por exemplo, de forma que um sólido conhecimento sobre segurança da informação é indispensável. Posto isso, é importante ressaltar que o pensamento computacional funciona para ambas as partes: aqueles que desejam atacar e aqueles que desejam se proteger.

Neste capítulo, vamos tratar dos princípios de segurança da informação e explicar como eles estão relacionados ao pensamento computacional. Além disso, vamos apresentar as principais ameaças enfrentadas pela segurança, bem como os crimes cibernéticos mais comuns. Por fim, vamos descrever as principais técnicas para o gerenciamento da segurança da informação.

Pilares da segurança da informação

Na Era Digital, informações são ativos organizacionais valiosos, então protegê-las é fundamental. Assim, uma segurança da informação bem estruturada é um ponto crucial para a sobrevivência da organização. Os ativos da tecnologia da informação das empresas envolvem dispositivos de computação, infraestrutura, aplicações, serviços e seus dados, sejam eles em transmissão ou armazenados. Todos esses ativos exigem proteção contra uma grande diversidade de ameaças, acidentais ou deliberadas, necessitando de diferentes controles de segurança.

Dessa forma, **segurança da informação** é um conjunto de estratégias utilizadas para o gerenciamento de processos, de ferramentas e de políticas necessário para a prevenção, a detecção, a documentação e o combate de ameaças, de acessos, de alterações ou de destruições não autorizados às informações, sejam elas digitais ou não. Há outras definições de segurança da informação, como, por exemplo, esta, dada por Coelho, Araújo e Bezerra (2014, p. 2):

> Segurança da informação compreende a proteção de informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança. Todos esses controles necessitam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados para que assegurem que os objetivos do negócio e a segurança da informação da organização sejam atendidos.

De forma complementar, Riley e Hunt (2014) explicam que os sistemas de segurança são procedimentos, políticas, dispositivos e mecanismos projetados para a mitigação de vulnerabilidades de modo explícito. Em outras palavras, de acordo com o National Institute of Standards and Technology (BARKER, 2003, p. 15) "[...] o termo 'segurança da informação' significa proteger a informação e os sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de fornecer integridade, confidencialidade e disponibilidade", e esses são os três pilares da segurança da informação, os quais abordaremos em detalhes a seguir.

Confidencialidade

A confidencialidade diz respeito ao acesso de dados e de informações somente por pessoas, processos ou dispositivos autorizados. A confidencialidade envolve tanto dados armazenados quanto os que estão sendo transmitidos,

que devem sempre estar protegidos também durante a transmissão. Senhas, criptografia, autenticação e defesa contra ataques de penetração são algumas técnicas que podem ser utilizadas de modo a preservar a confidencialidade.

Integridade

Riley e Hunt (2014) assumem que, em um mundo conectado à internet, as informações se movem livremente e, por isso, é necessário associar responsabilidades. Dessa forma, as informações possuem duas partes: os dados armazenados e o responsável por esses dados, podendo ser uma pessoa, um processo ou um dispositivo. Quando um *e-mail* ou um pacote de dados é enviado via internet, é importante que o conteúdo seja conhecido, bem como quem os enviou. Isso resulta em dois tipos de integridade, a de dados e a de propriedade, sendo as duas fundamentais para o estabelecimento de integridade total.

A **integridade de dados** visa garantir o estado original dos dados, ou seja, assegurar que as informações acessadas não foram modificadas, destruídas ou sofreram fraudes. As técnicas utilizadas para garantir a confiabilidade são o caminho para a integridade, pois um invasor não será capaz de modificar o que não conseguir acessar. Portanto, para que uma informação seja íntegra, primeiramente deve ser confiável.

A **integridade de propriedade** é um pouco mais complicada, porque, em alguns casos, a informação pode ser anônima, ou pode haver várias pessoas reivindicando sua propriedade, o que torna impossível a integridade de propriedade. Posto isso, Riley e Hunt (2014) garantem que sistemas de segurança eficientes dependem de conhecer o proprietário dos dados. Usuários, processos e dispositivos que possuem ativos devem ter uma identidade única dentro dos sistemas de segurança, como: endereços de *e-mail*, identificação de usuário e endereços de IP (Internet Protocol) dos dispositivos.

Existem ferramentas que podem verificar a integridade dos dados, como ferramentas de controle de versão de arquivo e o *hash*, que é um algoritmo que lê o arquivo completo e gera um código; caso o arquivo seja modificado, o código será alterado. Além disso, é necessário possuir serviços de *backups* confiáveis, de modo que a versão original dos dados possa ser restaurada caso ocorram alterações ou exclusões acidentais.

Disponibilidade

A disponibilidade é a garantia de que os dados estarão disponíveis sempre que necessário, uma vez que uma informação indisponível é uma informação inútil. Dessa forma, como pilar de segurança, a usabilidade foi projetada para que todos os usuários que possuam permissões apropriadas consigam acessar as informações a qualquer momento, garantindo sua acessibilidade. No entanto, esse princípio também depende de alguns fatores para que seja eficaz, como funcionamento apropriado da rede e eficácia dos sistemas, sendo fundamental uma manutenção adequada de infraestrutura. Planos de recuperação de desastres e *backups* eficientes são essenciais para que as informações se mantenham disponíveis mesmo em casos de incidentes.

Exemplo

Um exemplo do papel da confidencialidade, integridade e disponibilidade em segurança é o envio de *e-mails* por meio de um dispositivo móvel, como um *smartphone*, fazendo uso da rede 4G. Quando um *e-mail* é enviado, espera-se que apenas o destinatário o receba e tenha acesso ao conteúdo, de modo a garantir sua confidencialidade. Outra questão é referente à integridade, que as informações sejam enviadas de forma correta, sem que sejam interceptadas e alteradas, por exemplo, ou que não cheguem corrompidas a seu destino, garantindo que a transmissão seja precisa. Já a disponibilidade depende das torres da operadora de telefonia, que devem estar funcionando de modo correto, necessitando que as linhas de transmissão tenham capacidade e cobertura de telefone eficientes.

O pensamento computacional requer que novos problemas sejam analisados de maneira cuidadosa. Para considerar que realmente existe a proteção, a informação deve ser confiável, ter integridade e estar disponível. Portanto, pela definição de cada um dos pilares, é possível observar que eles são codependentes, ou seja, os três devem estar bem alinhados e trabalhando juntos, pois, caso algum deles seja comprometido, toda a segurança será comprometida, não havendo, assim, segurança da informação.

Ameaças à segurança

Até o surgimento das redes, a segurança da informação não era uma grande preocupação. Com o uso da internet, foi necessário mudar de pensamento, pois ela apresenta inúmeras vulnerabilidades de segurança. Além de ser uma portadora para atacantes, ela conecta um computador a outros ou a servidores, os quais podem ter suas próprias falhas, seja de *software* e falta de segurança física. Outro ponto de vulnerabilidade são os protocolos de comunicação, dos quais a internet depende. Muitos não são projetados para serem especialmente seguros, e, ainda, as redes podem ser configuradas de modo a deixar possíveis brechas de segurança. Todas essas questões são extremamente relevantes, pois, graças à internet, que também trouxe diversas vantagens, um invasor, mesmo que esteja em outro país, pode conseguir acessar as informações de outrem, roubá-las ou danificá-las (RILEY; HUNT, 2014).

De fato, os atacantes possuem mais vantagens do que um analista de segurança, porque eles não seguem regras na hora de realizar um ataque; escolhem quais vulnerabilidades vão explorar e criam ataques de acordo com o que desejam. Enquanto isso, os analistas devem seguir todos os procedimentos de acordo com o que é permitido, fazendo o possível para identificar e mitigar todas as vulnerabilidades existentes em sua rede. Além disso, os analistas de segurança conseguem se proteger apenas de ataques já existentes, daqueles que se tem conhecimento, o que facilita o "trabalho" de invasores que tenham desenvolvido um novo ataque (RILEY; HUNT, 2014).

À medida que o computador foi se tornando essencial para comércio, o entretenimento e até o governo, cresceu, em uníssono, o número de ataques a sua segurança. O **cibercrime**, ou crime cibernético, é todo crime praticado *on-line* ou principalmente *on-line*. Os cibercriminosos utilizam computadores como instrumentos para fins ilegais como cometer fraudes, tráfico de pornografia infantil, roubo de identidade, violação de privacidade, entre outros (DENNIS, 2019).

Os autores Riley e Hunt (2014) e o *site* High Security Center (2020) apresentam algumas das principais ameaças virtuais. Vejamos cada uma em detalhes a seguir.

Ataques direcionados

Esse tipo de ataque utiliza informações específicas de uma empresa, de modo a executar o ataque. O atacante estuda muito bem seu alvo e faz uso da engenharia social, com o intuito de induzir as vítimas ao erro, como

fazer depósitos em uma conta, por exemplo. Esses ataques são persistentes, ou seja, os invasores fazem o possível para que o ataque continue após a penetração inicial.

O *business e-mail compromise* (mais conhecido como BEC) é um exemplo de ataque direcional e também é uma das principais ameaças virtuais. Nesse caso, o atacante estuda tão bem a organização a ponto de identificar um profissional de alto cargo e algum funcionário da área financeira, por exemplo, responsável por pagamentos. O invasor então frauda o *e-mail* desse profissional de alto cargo e envia uma solicitação, ao colaborador do financeiro, de transferências de alto valores para determinadas contas, que acaba realizando os pagamentos por ser algo do cotidiano.

Ameaças persistentes avançadas

As ameaças persistentes avançadas (ou APT, do inglês *advanced persistent threats*) usam técnicas de *hacking* contínuas (tentativa de explorar sistemas de computadores com propósitos ilícitos), clandestinas e sofisticadas, que buscam obter o acesso a um sistema e manter-se dentro dele por um longo período. Normalmente, esses ataques são direcionados a alvos como o governo ou grandes organizações. São usadas técnicas como *malwares* e *phishing*, por exemplo, para obter acesso à rede desejada.

Kaspersky (2021) afirma que o propósito de um APT é obter acesso contínuo aos sistemas por meio de cinco estágios:

1. obter o acesso, normalmente por meio de um arquivo infectado;
2. estabelecer ponto de apoio, implementando *malwares* que permitem a criação de uma rede de *backdoors* (o que permite o retorno do atacante remotamente ao computador da vítima sem que seja notado), em que os *malwares* geralmente empregam técnicas como reescrever códigos que ajudam os *hackers* a encobrir seus rastros;
3. aprofundar o acesso por meio de quebras de senhas, com o intuito de obter acesso aos direitos de administrador na rede;
4. mover-se lateralmente com os direitos de administradores, de forma a ser possível acessar outros servidores e outras partes da rede;
5. olhar, aprender e permanecer, ou seja, uma vez dentro do sistema, os atacantes podem obter um entendimento completo sobre o funcionamento de seu alvo e suas vulnerabilidades, mantendo o processo em execução indefinidamente ou até atingir seus objetivos.

Ataques a dispositivos IoT

A Internet das Coisas (ou IoT, do inglês Internet of Things) está em crescimento e a cada dia surgem mais dispositivos IoT que trazem inúmeras vantagens. Porém, a maioria desses dispositivos apresenta um *hardware* muito limitado, não possuindo um sistema de segurança robusto. Dessa forma, os atacantes aproveitam para invadir dispositivos IoT para copiar ou comprometer os dados transmitidos por eles, possibilitando a espionagem industrial. Além disso, também podem utilizá-los somente como porta de entrada para conseguir invadir uma rede por completo.

DDoS-for-hire (DDoS de aluguel)

O *DDoS-for-hire* são *botnets* (*softwares* que se propagam de forma automática por meio da exploração de vulnerabilidades nos sistemas) vendidos pelos *hackers*, que já realizam um ataque DDoS por conta própria, o que facilita o acesso de *hackers* iniciantes a ferramentas mais poderosas e simples de usar.

Os ataques de negação de serviço distribuído (DDoS, ou *distributed denial of service*) são utilizados para interromper completamente o serviço de um sistema. Para isso, o atacante utiliza um computador mestre, que escraviza vários outros e faz com que todos acessem o sistema desejado ao mesmo tempo, de maneira ininterrupta. Como os servidores geralmente possuem um número limitado de acessos simultâneos, acabam sendo interrompidos por completo.

Engenharia social

O ataque de engenharia social apenas engana a vítima, não necessitando da utilização de *softwares* maliciosos ou de conhecimentos mais profundos sobre ataques. Ela utiliza uma das maiores fraquezas dentro de uma organização, que é o fator humano. O criminoso obtém a confiança da vítima para extrair dados pessoais e até dados confidenciais das organizações, por meio de *e-mails*, por exemplo.

Malwares

São códigos maliciosos que se infiltram nos equipamentos de forma ilícita. Seu objetivo é destruir, alterar ou roubar dados. Eles podem comprometer um computador por meio da exploração de vulnerabilidades, da execução

de mídias removíveis infectadas, do acesso a páginas maliciosas na *web*, da execução de arquivos maliciosos que podem ter sido obtidos em anexos de *e-mail*, da ação direta dos atacantes, que invadem o equipamento e incluem arquivos contendo o código malicioso, entre outras formas. Os *malwares*, após executados, possuem acesso a todos os dados armazenados no equipamento infectado e, de acordo com as permissões das vítimas, conseguem executar ações na rede (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2012).

Ransomware

O *ransomware*, ao infectar um computador, realiza o sequestro dos dados, ou seja, criptografa todos os dados do equipamento, de um sistema de dados ou até de uma rede inteira, impedindo o acesso aos arquivos. Os criminosos, para liberar a chave, pedem pagamentos, geralmente em criptomoedas. A infecção pode ocorrer por meio de *links* em *e-mail* de *phishing* (prática cujo objetivo, em geral, é roubar dados de usuários por meio de *links* em *e-mail*) ou de arquivos em anexos, por exemplo.

Saiba mais

No final de 2020, o Superior Tribunal de Justiça (STJ) foi vítima de um ataque de *ransomware*. Todos os ministros, servidores e funcionários do STJ foram recomendados a não acessar os computadores ligados à rede do tribunal. Além do STJ, o Ministério da Saúde também perdeu acesso a seus sistemas de comunicação no mesmo dia. A Secretaria de Economia do Distrito Federal também informou que identificou uma tentativa de invasão à rede GDFNet, que pertence ao Governo do Distrito Federal. Desesperados, sem saber o que fazer, decidiram o extremo: remover seus servidores do ar por precaução e falta de ferramentas para se proteger (PETRY, 2020).

Spoofing

O *spoofing* é um ataque de engenharia social. Ocorre quando o cibercriminoso se passa por outra pessoa, uma pessoa conhecida, para obter informações pessoais, de modo a realizar fraudes. Pode ocorrer através de uma mensagem de e-mail com um endereço de retorno falsificado ou um pacote de rede com um endereço de IP falsificado, que redireciona o tráfego de internet para a página maliciosa.

Sniffer

É um programa de computador projetado para capturar informações de rede em tempo real e enviá-las ao invasor. Ele captura todos os dados que entram ou saem do equipamento infectado.

Além desses cibercrimes, também existem duas técnicas menos sofisticadas de violação de confiabilidade e que não exigem qualquer tipo de conhecimento sobre ataques: o *shoulder surfing* (surfar sobre os ombros) e o *dumpster diving* (mergulho no lixo). O surfe sobre os ombros ocorre quando uma das partes consegue observar uma pessoa digitando seus dados no teclado do computador, conseguindo, assim, roubar seus dados de usuário. Já o mergulho no lixo é o ato de roubar materiais confidenciais que seriam descartados.

Gerenciamento de segurança da informação

O pensamento computacional é uma forma de pensar e resolver problemas por meio de computadores. Quando esses dispositivos se conectam a uma rede, ficam sujeitos às ameaças citadas na seção anterior. Portanto, é necessário um gerenciamento de segurança eficiente. Subramanian *et al.* (2010) afirmam que esse gerenciamento envolve a proteção do acesso à rede e dos dados armazenados e transmitidos pela rede.

Para um gerenciamento eficiente, é fundamental a aplicação de algumas técnicas e estratégias de segurança, com o objetivo de mitigar as ameaças. Riley e Hunt (2014) citam algumas dessas técnicas, detalhadas a seguir.

Autenticação

Nos sistemas de computadores, quatro fatores podem ser utilizados para autenticar:

1. algo que o sujeito sabe;
2. algo que o sujeito possui;
3. algo que o sujeito é;
4. lugar onde o sujeito está localizado.

"Sujeito" se refere à pessoa, ao processo ou ao dispositivo.

Para qualquer sistema de segurança, a autenticação é um dos principais fatores, pois é por meio dela que o sistema verifica a identidade do usuário.

Quando a autenticação é bem sucedida, diminui os riscos de roubo de identidade e de ataques de falsificação. A maneira mais comum de autenticação é a utilização de usuário e senha, que, teoricamente, são informações individuais e confidenciais, ou seja, apenas o sujeito que deseja autenticar deve ter conhecimento de tais informações.

A segurança física depende do segundo fator, algo que o sujeito possui. *Tokens* e *smartcards*, que são dispositivos que devem ser conectados fisicamente aos computadores para que o usuário seja identificado e autenticado aos sistemas, estão sendo muito utilizados pelas empresas como forma de autenticação.

O terceiro fator é referente a algo que o sujeito é. Nesse caso, a autenticação é realizada por meio de características humanas reais, sendo a biometria do usuário a mais utilizada. A autenticação por biometria funciona por meio da impressão digital do usuário, que o identifica e permite seu acesso. Caixas eletrônicos e *smartphones*, por exemplo, têm aderido cada vez mais a essa técnica de segurança.

O último fator não é muito utilizado, pois conhecer a localização do sujeito não é o suficiente para autenticar. Porém, ela pode ser usada como parte de autenticação de um *e-mail*, por exemplo. Quando recebido de um destinatário desconhecido, é possível verificar o país de origem por meio de um sufixo, que geralmente é incluído como parte do endereço de *e-mail*.

A autenticação em dois fatores é um mecanismo ainda mais seguro. Isso significa que é utilizada uma combinação de dois dos fatores, considerando apenas os três primeiros. Por exemplo, o *token*: além de ser necessário possuí-lo fisicamente, o sujeito também precisa saber o código de acesso, pois só assim será autenticado.

Na internet, esse processo é diferente. Cada computador possui um número exclusivo, que é o endereço MAC (*media access control*, ou controle de acesso de mídia), definido já em sua fabricação. Quando um computador transmite dados em uma rede, ele é identificado por seu MAC. Outro identificador exclusivo de um computador é o número do IP, atribuído pelos administradores de rede ou automaticamente por dispositivos que o distribuem.

Autorização

Nos sistemas de segurança, diferentes usuários possuem diferentes autorizações de acesso. Dentro de uma organização, por exemplo, colaboradores do setor financeiro não devem possuir acesso aos arquivos do setor de recursos

humanos. Dentro de uma rede, essas autorizações são dadas de acordo com o nome de usuário, que são nomes únicos definidos para cada usuário.

Existem diferentes classes de autorização em informações eletrônicas, que são: leitura, gravação, proprietário e execução. Quem possui autorização para leitura somente pode inspecionar o documento, já a permissão de gravação autoriza a alterar ou atualizar o documento. O proprietário geralmente é apenas um e consegue excluir, renomear e até alterar permissões de acesso ao documento. Já a autorização de execução diz respeito a *softwares* de computador e o nome já leva a entender que essa autorização é para que o usuário autorizado possa executá-los. Essas autorizações podem ser concedidas individualmente ou a grupos de usuários.

Criptografia

Quando um invasor consegue acesso a dados ou os intercepta durante uma transferência, consegue obter acesso a todos os conteúdos que ali estão armazenados, podendo roubar tais informações ou simplesmente alterá-las, afetando sua integridade. Para evitar isso, é necessário o uso de criptografia. A criptografia é um processo que converte dados para um formato irreconhecível, de modo a proteger informações confidenciais, sendo possível que somente as partes autorizadas possam visualizá-las. Ou seja, é utilizado um algoritmo que transforma as informações, tornando-as ilegíveis para qualquer usuário que não seja autorizado, pois os dados codificados só podem ser descriptografados com uma chave. A criptografia pode ser com chave simétrica ou assimétrica.

De acordo com Vallim (2019), a **criptografia de chave simétrica** usa a mesma chave para criptografar e descriptografar mensagens. Portanto, algoritmos simétricos são mais simples do que algoritmos assimétricos e têm maior velocidade de processamento, o que apresenta grandes vantagens quando grandes quantidades de dados estão envolvidas. No entanto, como todos os envolvidos precisam conhecer a mesma chave, esse método apresenta lacunas no processo de comunicação criptográfica. Uma vez que apenas uma chave é usada para cifrar e decifrar a mensagem, o criador da mensagem não pode ser identificado, o que permite que um terceiro que conheça a chave altere a mensagem sem que o usuário no destino fique ciente de que algo aconteceu durante a transmissão.

Já a **criptografia de chave assimétrica**, também chamada de criptografia de chave pública, usa duas chaves: uma para criptografar e outra para descriptografar. A chave usada para criptografar é secreta e apenas o criador

da mensagem a conhece, por isso é chamada de privada, enquanto a chave usada para descriptografar é pública e todos sabem. Essas duas chaves são geradas e associadas simultaneamente pelo algoritmo. Portanto, apenas o destinatário poderá acessar o conteúdo da mensagem, garantindo sua autoria. Embora exija mais processamento do que uma chave simétrica, essa criptografia pode garantir a confidencialidade e autenticidade da mensagem protegida (VALLIM, 2019).

Firewall

O *firewall* é um dispositivo de segurança de rede responsável pelo monitoramento do tráfego de entrada e saída da rede. Atua como um filtro, decidindo se permite ou bloqueia determinado tráfego, e age com base em um conjunto predeterminado de regras de segurança.

Firewalls podem ser em forma de *hardware* ou apenas de *software*. Como dispositivo físico, ele é posicionado entre os computadores e a internet, de maneira que todo o tráfego de internet passe primeiro pelo *firewall* para ser filtrado.

Os sistemas de computador possuem *firewalls* já incorporados. Esses *firewalls* em formato de *software* fazem a inspeção das mensagens no ponto de conexão de rede do computador. Quando a mensagem chega à placa de rede do equipamento, imediatamente o *firewall* age, definindo se o tráfego é malicioso ou não, realizando os bloqueios quando necessário.

O dispositivo físico é mais sofisticado do que o *software* e, consequentemente, mais seguro. A maioria das organizações opta pelo *hardware*, utilizando-o para proteger toda a rede e seus dispositivos com acesso à internet. Esses equipamentos são complexos, por isso é necessária mão de obra especializada para sua instalação e configuração, pois seu funcionamento só será eficiente se for configurado de maneira correta.

São configurados com listas de controle de acesso (ACLs, do inglês *access control lists*), em que se define o que pode passar pelo *firewall* e o que deve ser bloqueado. Porém, é uma tarefa complexa. Uma das técnicas utilizadas para essa definição é o uso do número IP dos computadores que enviam e recebem as mensagens. Isso pode ser feito com base em uma lista negra, que é uma lista que contém os números de IPs atribuídos a ataques. Essa lista deve ser distribuída para o *firewall* e atualizada de maneira regular.

O *firewall* também pode restringir tráfego de saída, evitando que usuários acessem páginas que podem representar riscos à rede.

Antivírus

A expressão **vírus de computador** se refere à coleção de diversos *malwares* que podem infectar os dispositivos. São *softwares* maliciosos que podem causar comportamentos inesperados no equipamento infectado ou apagar todo o conteúdo do disco rígido. Eles podem se propagar de um computador a outro pela rede ou por compartilhamento de dispositivos de armazenamento portáteis, como *pen drives* e discos externos, por exemplo.

Para mitigar esse tipo de infeção, existem os *softwares* antivírus. Esses *softwares* devem ser executados nos equipamentos para realizar verificações em busca de arquivos maliciosos. As verificações podem ocorrer automaticamente, quando novos arquivos são detectados, de maneira programada, para ocorrer uma vez ao dia, por exemplo, ou manualmente, sempre que o usuário desejar.

Para essas detecções, os antivírus utilizam listas que armazenam sequências de bits, ou seja, uma assinatura de bit exclusiva de um vírus, sua identidade. Quando o antivírus identifica uma assinatura de bit que corresponde a um vírus conhecido, já considera o arquivo infectado, podendo ser excluído automaticamente ou notificando para que o usuário tome alguma ação.

Em geral, esses *softwares* são eficientes, porém, mas vírus recém-lançados tornam-se um problema, pois pode demorar um tempo considerável até que suas assinaturas de bit sejam conhecidas e atualizadas nos antivírus.

Atualização de *software*

Tanto *firewalls* quanto antivírus devem estar em constante atualização, para que possam cumprir seus papéis de maneira eficiente; caso contrário, tornam-se vulnerabilidades. Dessa mesma forma, os computadores também devem ser atualizados regularmente, de modo a evitar que ocorram falhas de *software*, que também se tornarão vulnerabilidades do sistema.

Geralmente, as empresas responsáveis pela criação de *softwares* são também responsáveis por desenvolverem atualizações sempre que surgirem vulnerabilidades nos sistemas, sendo obrigadas a corrigir a falha de *software* lançando uma nova versão sem os problemas detectados. Essas atualizações são entregues via internet e, em alguns casos, são realizadas automaticamente; porém, em outros, exigem que o usuário solicite a verificação de atualização manualmente.

Backups

Realizar *backups* regularmente é uma técnica de segurança fundamental. Supondo que, mesmo com todos os cuidados, utilizando todos os procedimentos possíveis para garantir uma rede segura, seu equipamento sofra um ataque e seus arquivos sejam danificados, ou até mesmo o disco inteiro apagado, se existir um *backup*, que tenha sido realizado em um dispositivo portátil ou em servidor, será possível recuperar os principais dados.

Posto isso, o *backup* ocorre quando os arquivos do computador são copiados para algum outro local, sendo necessário que isso seja realizado o mais frequentemente possível, de modo a manter o *backup* sempre atualizado. Em organizações, geralmente o administrador de rede configura para que sejam realizados *backups* diariamente, salvando todos os arquivos que estejam compartilhados no servidor; mesmo assim, é recomendado que os usuários realizem seus *backups* individualmente, pois muitas informações importantes podem estar armazenadas localmente. Dessa forma, é possível entender sua importância para a segurança de uma rede.

Arquivos de *log*

Os arquivos de *log* são os responsáveis por registrar eventos que ocorrem durante o uso do computador como: usuário que fez *login*, arquivo criado ou lido e *e-mail* enviado ou recebido. Os sistemas registram alguns *logs* por padrão, mas as configurações podem ser alteradas para registrar o que os usuários desejam incluir nos arquivos de *log*.

Por meio desses arquivos, é possível identificar qual equipamento e qual usuário foram responsáveis pela realização de um crime, por exemplo. Também é importante porque nem sempre os ataques ocorridos em uma empresa são executados por alguém de fora; muitos casos envolvem usuários internos. Assim, analisando os *logs*, é possível identificar de onde o ataque foi efetuado.

Sistemas de detecção de intrusão

Os sistemas de detecção de intrusão, ou IDSs (do inglês *intrusion detection systems*) são dispositivos, podendo ser *hardware*, *software* ou uma combinação de ambos, responsáveis pelo monitoramento das atividades de redes ou sistemas. Esses dispositivos podem ser baseados em rede ou *host*. O **IDS baseado**

em rede (NIDS, do inglês *network intrusion detection systems*) é posicionado na rede para monitorar o tráfego. Essa análise é realizada se baseando em padrões de comportamentos esperados pela rede (como a banda utilizada, protocolos, portas e conexões mais comuns) ou em assinaturas, realizando comparações com assinaturas e atributos de ameaças já conhecidas. Já o **IDS baseado em host** (HIDS, do inglês *host-based intrusion detection system*) detecta não apenas ameaças externas, mas também comportamentos suspeitos de usuários internos, como, por exemplo, quando ocorrem falhas de autenticação, tentativas de alterações em processos do sistema, análise de *logs*, modificações em privilégios de usuários e tentativas de acesso a arquivos não autorizados. Em ambos os tipos, o dispositivo gera alertas aos administradores ou toma contramedidas reativas quando alguma atividade suspeita é identificada, de modo que as ameaças sejam barradas antes que a rede seja prejudicada (VELHO, 2016).

Fique atento

O fator humano é o elo mais fraco de qualquer organização: pessoas são suscetíveis a erros, a realizar acessos indevidos e a serem vítimas da engenharia social. Segundo uma pesquisa realizada em 2018 pelo High Security Center (2020), 57 milhões de brasileiros acessaram *links* maliciosos naquele ano, 55% de todos os *e-mails* recebidos eram *spam* e 90% dos ciberataques utilizaram *e-mails* de *phishing*. Portanto, é de extrema importância investir na educação dos colaboradores, realizando treinamentos de segurança regularmente, orientando-os sobre os riscos, sobre como é possível evitá-los e sobre as políticas de segurança aplicadas, como a obrigatoriedade da alteração de senha em períodos predeterminados, além da exigência de maior complexidade, utilizando letras, números e caracteres especiais. Outras recomendações importantes incluem não digitar dados de usuário, como a senha, na presença de outras pessoas e procurar não anotar senha em lugares que possam ser acessados por terceiros, não acessar *links* de remetentes desconhecidos (e até mesmo de conhecidos) antes de ter certeza de que seja um *link* real, pois podem ter sidos enviados por um invasor, etc.

Nenhuma rede é totalmente segura. No entanto, quando implementado o conjunto de técnicas de segurança citadas anteriormente, as ameaças podem ser mitigadas, tornando as redes menos vulneráveis a ataques.

Referências

BARKER, W. C. *Information security*. 2003. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf. Acesso em 29/12/2020. Acesso em: 27 jan. 2020.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. *Cartilha de segurança para internet*. São Paulo: CERT.br, 2012. (*E-book*).

COELHO, F. E. S.; ARAÚJO, L. G. S. de; BEZERRA, E. K. *Segurança da Informação*: NBR 27001 e NBR 27002. Rio de Janeiro: RNP, 2014.

DENNIS, M. A. Cybercrime. *In*: BRITANNICA, 2019. Disponível em: https://www.britannica.com/topic/cybercrime. Acesso em: 27 jan. 2020.

HIGH SECURITY CENTER. *Principais ameaças em 2020*. 2020. Disponível em: https://www.hscbrasil.com.br/principais-ameacas-virtuais/. Acesso em: 27 jan. 2020.

KASPERSKY. *What is an advanced persistent threat (APT)?* 2021. Disponível em: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats. Acesso em: 27 jan. 2020.

PETRY, G. M. *STJ é vítima de ransomware e tem seus dados e os backups criptografados*. 2020. Disponível em: https://thehack.com.br/stj-e-vitima-de-ransomware-e-tem-seus--dados-e-os-backups-criptografados/. Acesso em: 27 jan. 2020.COELHO, F. E. S. et al. Segurança da Informação: NBR 27001 e NBR 27002. Rio de Janeiro: RNP, 2014.

RILEY, D. D.; HUNT, K. A. *Computational thinking for the modern problem solver*. Boca Raton: CRC Press, 2014.

SUBRAMANIAN, M. *et al*. *Network management*: principles and practice. India: Pearson Education, 2010.

VALLIM, A. P. de A. *Forense computacional e criptografia*. São Paulo: Senac, 2019.

VELHO, J. A. *Tratado de computação forense*. Campinas: Millennium, 2016.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Crimes digitais

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Reconhecer as características de um crime digital.
- Identificar os tipos mais comuns de crimes digitais.
- Apresentar os princípios de investigação de crimes digitais.

Introdução

Os crimes digitais passaram a fazer parte do dia a dia das pessoas a partir do uso da Internet pela população e também pelas grandes organizações. Como em todos os meios, há oportunidade de os indivíduos realizarem crimes contrariando a lei em busca de benefícios próprios.

Os crimes digitais estão ganhando volume devido ao uso massivo da rede de computadores no cotidiano das pessoas. As ações — como estelionato, um crime que existe desde o início da humanidade — se tornaram cada vez mais frequentes no ambiente digital, principalmente pelas redes sociais, ganhando volume estrondoso e gerando inúmeros prejuízos para a sociedade e também para as empresas.

Observamos também um volume crescente de crimes de calúnia, difamação e injúrias, a partir de encorajamento das pessoas nas redes sociais, novamente embasados pela falsa percepção de impunidade.

Neste capítulo, você vai ver como os crimes são caracterizados, os tipos de crimes digitais e os princípios de investigação de crimes digitais.

1 Características de um crime digital

Com o nascimento da Internet nos EUA na década de 1960, que tinha um ideal bélico criado pela Defense Advanced Research Projects Agency para inibir intervenções em suas comunicações pela extinta União Soviética, passamos a ter um sistema de informação interligado, sem localização física ou central específica.

Em 1970, foi criado o par de padrões Transfer Control Protocol/Internet Protocol (TCP/IP — Protocolo Controle de Transferência/Protocolo de Internet), permitindo a comunicação entre usuários. Na década de 1980, foi criado o conceito de Internet, por meio da ampliação do uso da rede para ações comerciais.

A partir de 1990, a rede *web* ganhou notoriedade, passando a ser um dos principais meios de comunicação. Esse novo modelo trouxe com ele um universo amplo para disponibilização de informações e um novo modelo de convivência na sociedade, no qual podemos conversar com qualquer pessoa a qualquer momento em qualquer lugar do mundo.

O uso dessa rede de computadores abriu uma importante porta para os crimes realizados na rede, chamados de crimes digitais. Na década de 1970, foi criado o termo *hacker*, que é o indivíduo capaz de promover a invasão de sistemas privados a partir de conhecimentos técnicos.

Os crimes digitais realizados pelas redes públicas, privadas ou domésticas podem atingir um ou vários indivíduos. Uma característica marcante nesse tipo de crime é a exponencialidade das ações, afinal, um *software* malicioso utilizado para o furto de dados pode obter dados de vários clientes de uma organização.

Segundo estudo da Escola de Magistrados da Justiça Federal da 3ª Região (BRASIL, 2017, p. 19):

> [...] Com a popularização do acesso à Internet nos últimos anos, os crimes digitais no Brasil alcançam números assustadores. De acordo com a SaferNet (2017), que controla a Central Nacional de Denúncias, mais de 115 mil denúncias envolvendo exclusivamente crimes contra direitos humanos foram recebidas e processadas no ano de 2016.

Com a evolução da Internet, os crimes cibernéticos passaram a ser tão comuns que foram criadas no Brasil delegacias próprias para a realização desse tipo de denúncia, assim como mudanças na legislação, criando um recente amparo legal para julgar e punir crimes dessa natureza. Para entendermos melhor os crimes digitais, é importante entender como a Internet é segmentada:

- ***Surface web*** (*web* superficial) — é aquela na qual navegamos e acessamos *sites* de empresas, bancos, redes sociais, entre outros. Utilizamos navegadores como Google Chrome e buscadores como Google, Bing, entre outros, para realizar nossas pesquisas. Apesar da percepção que

existe um volume estrondoso de dados nesse segmento da rede, há análises de volumes de acessos que afirmam que apenas 4% de toda a informação circulada está na parte da *surface web*, conforme consta na pesquisa realizada pela empresa Experian (SIRUL, 2018, documento *on-line*, tradução nossa):

> [...] Se você é como a maioria das pessoas, é aqui que você passa a maior parte do tempo — fazendo compras *on-line*, pesquisando informações e compartilhando fotos e vídeos nas mídias sociais. No entanto, isso representa apenas cerca de 4% da Internet.

- ***Deep web*** — ao contrário da *surface web*, é composta por *sites* não indexados, portanto, não é possível encontrá-los nos canais de busca, como o Google. As informações presentes lá só podem ser acessadas se você realmente procurar. Quem acessa a *deep web* utiliza redes criptografadas, que ocultam a sua identidade. Esses sistemas funcionam com navegadores tradicionais, como Chrome, Firefox, entre outros, porém sem endereço IP e dados do usuário, que dificultam a identificação de quem está navegando. Nem todas as pessoas que navegam pela *deep web* cometem atos ilegais, algumas apenas querem ficar no anonimato, muito comum no mundo corporativo de grandes organizações e também utilizada por órgãos governamentais, entretanto, não podemos descartar que essa parte da Internet é utilizada sim para cometer crimes digitais.
- ***Dark web*** — também conhecida como zona escura da Internet, a criptografia é extremamente complexa, permitindo que apenas usuários que conheçam esse tipo de criptografia cheguem até ela. A *dark web* representa uma pequena parte da *deep web*, entretanto, é nesse espaço da rede que ocorrem os crimes digitais, como troca de informações ilegais, tráfico de drogas, ações de *hackers*, pedofilia, pornografia, entre outros crimes. Esse tipo de crime ocorre já que nesse ambiente o anonimato é garantido e a polícia tem dificuldades para descobrir quem é o responsável.

Apesar de a *surface web* ser um ambiente criptografado, permitindo uma melhor investigação e punição em casos de crimes, não impede a realização de uma extensa gama de crimes. Existem muitas infrações nessa parte da rede, principalmente crimes relacionados a fraudes, estelionato, calúnia e difamação, sendo estas duas últimas muito comuns nas redes sociais. A Figura 1 faz uma analogia entre os níveis de profundidade da *web* e um *iceberg*.

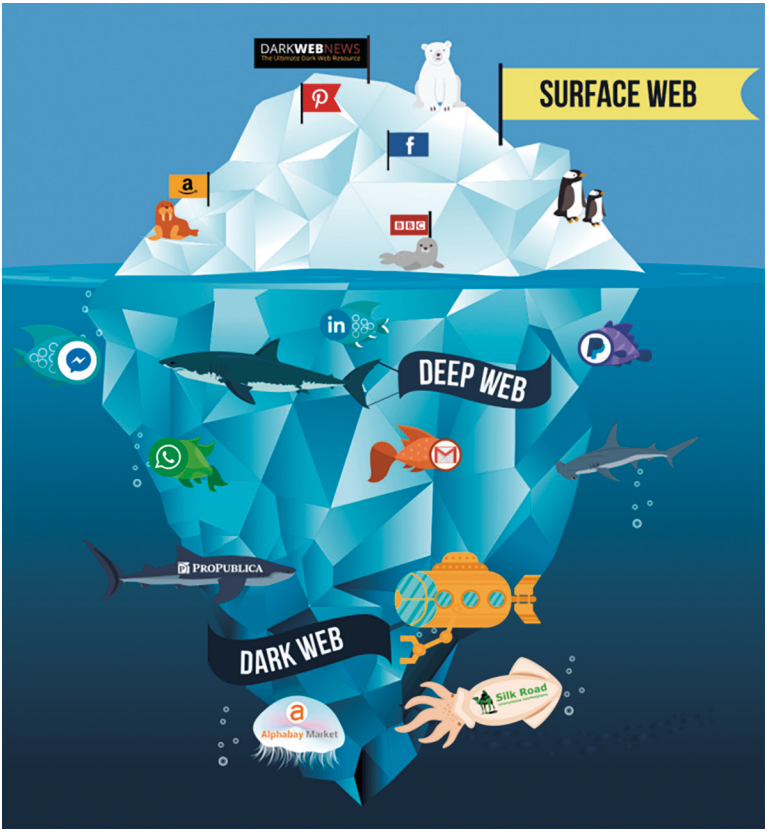

Figura 1. A *web* como um *iceberg*.
Fonte: Gogoni (2019, documento *on-line*).

A Internet é uma ferramenta-chave para as grandes organizações, permitindo a divulgação de seus produtos e aproximando o relacionamento com seus clientes. Entretanto, a Internet torna-se também uma grande preocupação em relação à segurança dos dados, tornando-se umas das maiores fontes de despesas com custos operacionais, como a compra e manutenção de ferramentas robustas para garantir a segurança das informações e a confiabilidade perante os clientes.

Nas últimas duas décadas, tivemos uma mudança cultural significativa no comportamento da sociedade a partir da criação das redes sociais. As redes sociais — pelas suas características de exposição impulsionada pelo uso de *smartphones* — trouxeram consigo um aumento nos crimes digitais a partir de uma exposição muito maior das pessoas. Outro crime que vem ganhando notoriedade com essa mudança comportamental é o aumento significativo de casos de injúrias e difamações, que estão cada vez mais comuns. Assim, o impacto que esse tipo de crime digital gera na vida das pessoas é gigantesco e desastroso.

Os usuários das redes sociais encaram suas convivências no mundo virtual como uma porta aberta para escrever o que bem entendem e realizar comentários extremamente prejudicais e ofensivos.

Saiba mais

Um estudo da Symantec, empresa do grupo Norton de segurança digital, indica que quase metade de todas as pessoas mundialmente conectadas à Internet fica feliz em contar mentiras sobre seus detalhes pessoais, incluindo nome, idade, situação financeira, estado civil, aparência e até mesmo sua nacionalidade. Além disso, um terço dos adultos já assumiu identidades falsas *on-line* — desde um nome falso até uma identidade totalmente fictícia. Os dados mostram que 33% dos adultos já utilizaram um nome falso e 45% mentiram sobre seus dados pessoais.

Os alemães são os melhores em fingir: mais da metade já adotou uma identidade falsa *on-line* ou já mentiu sobre detalhes pessoais *on-line* (53 e 51%, respectivamente). Mais da metade dos adultos chineses, brasileiros e indianos já admitiu ter mentido sobre as suas informações pessoais *on-line* (58, 56 e 55%, respectivamente).

Cerca de quatro em cada 10 italianos, brasileiros e neozelandeses já usaram identidades falsas *on-line* (41, 41 e 38%, respectivamente). As pessoas no Reino Unido sentem-se relutantes em fazer o mesmo — elas são as menos propensas a utilizar uma identidade falsa *on-line* (18%) ou mentir sobre as informações pessoais (33%).

2 Tipos mais comuns de crimes digitais

Com o crescente número de usuários na Internet, existe cada vez mais criminosos atuando na rede de computadores. Dessa forma, é muito importante entender os possíveis tipos de crimes que ocorrem na rede, ressaltando que os crimes digitais são ações que evoluem com muita velocidade. A cada novo dia, novos modelos de atividades ilícitas estão surgindo, incluindo as ações de mau comportamento dentro da rede, principalmente em redes sociais, transformando seus usuários em criminosos sujeitos a punições legais. Apresentamos a seguir alguns dos crimes virtuais mais comuns, que costumam ser praticados pela Internet:

- **Apologia ao crime** — incitar publicamente a prática de crime, fazer, publicamente (art. 287 "Apologia de fato criminoso ou de autor de crime" — Código Penal — Decreto-Lei nº. 2.848, de 7 de dezembro de 1940).
- **Aplicativos maliciosos (*malware*)** — são programas maliciosos instalados sem permissão do usuário, como vírus, para realização de furtos de dados pessoais, para fins fraudulentos.
- **Ato obsceno** — praticar ações de natureza sexual com ofensa ao pudor.
- **Calúnia** — atribuir sem provas a alguém uma ofensa que afete a sua dignidade ou acusar alguém de um crime.
- **Crimes virtuais contra mulheres** — envolvem casos de perseguições, ofensas, difamação, assédio e também a distribuição de fotos e vídeos pessoais.
- **Crimes de ódio** — são ataques racistas, de gênero, misóginos e até terroristas.
- **Difamação** — atribuir a alguém uma acusação pública que afete a sua reputação.
- **Divulgação de material confidencial** — expor publicamente dados de terceiros sem autorização (art. 153 "Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem" — Código Penal — Decreto-Lei nº. 2.848/1940).
- **Estupro virtual** — envolve coação para produção de conteúdo sexual sob ameaça de divulgação de fotos e vídeos.

- **Formulários falsos** — envio de mensagens de *e-mail* falsas para os usuários solicitando que seja preenchido um formulário, assim, os criminosos conseguem várias informações sobre os usuários, incluindo dados bancários.
- **Injúria** — atribuir a alguém uma ofensa desonrosa que afete a sua dignidade.
- **Lojas virtuais falsas** — é um golpe com a divulgação de ofertas falsas, com preços muito abaixo do preço real de produtos, no qual os usuários adquirem os produtos, realizam o pagamento, mas não recebem as mercadorias.
- **Pedofilia** — envolve armazenamento, produção, troca, publicação de vídeos e imagens contendo pornografia infantil ou do adolescente, cometido pela Internet.
- **Perfil falso** — refere-se usuários que criam identidade falsa na Internet para usar redes sociais, aplicar golpes ou realizar fraudes.
- ***Phishing*** — refere-se a conversas ou mensagens falsas com *links* fraudulentos.
- **Plágio** — é a cópia de informações veiculadas por terceiros sem a indicação da fonte.
- **Preconceito ou discriminação** — envolve utilizar *sites* da Internet ou redes sociais para opinar, de forma pejorativa e negativa, envolvendo assuntos como etnia, religião, opção sexual, raças, entre outros.
- ***Spam*** — são mensagens enviadas sem o consentimento do usuário.

Os crimes financeiros afetam inúmeros usuários da Internet, envolvendo desde ações que geram prejuízos individuais até ações que impactam ambientes corporativos, nos quais esse risco é muito maior, como o furto de dados confidenciais de seus clientes, o que poderá gerar prejuízos financeiros e à imagem da organização.

A Internet é um ambiente aberto, veloz e de fácil acesso. Vivemos em um período em que as crianças já nascem digitalizadas, assim, é nítida a velocidade na mudança dos hábitos da população em função dos usos de novas tecnologias. Por esse motivo, existe um árduo desafio na adaptação e definição de regras de boas condutas dentro do universo digital.

Assim, precisamos refletir sobre a importância da orientação e do acompanhamento dessas crianças, que não têm maturidade suficiente para se proteger de todos os perigos existentes no ambiente digital. Observamos mudanças na grade curricular do sistema de ensino, que passou a ser muito mais digitalizado, entretanto, essa digitalização ainda deixa muito espaço para crimes relacionados à pedofilia, que atinge um número imenso de crianças ao redor do mundo.

Além das redes sociais, o aplicativo WhatsApp, maior plataforma de mensagens utilizada massivamente ao redor do mundo, tem sido utilizado com muita frequência para aplicação de muitos dos crimes descritos. A Internet possibilita novas formas de interação social, sendo que esse novo modelo de relacionamento propicia golpes e o cometimento de crimes.

Uma recente pesquisa realizada pela PSafe, a desenvolvedora dos aplicativos dfndr, entre os dias 7 de maio e 22 de maio de 2019, revelou que um em cada cinco brasileiros já foi vítima de roubo de identidade na Internet, o que representa 24,2 milhões de potenciais vítimas em todo o País. As respostas à pergunta "Alguma das informações pessoais abaixo já foram usadas por alguém sem a sua permissão?" nessa pesquisa foram as seguintes (PAVÃO, 2019; PESQUISA..., 2019):

- 51,3% — número do telefone;
- 44,3% — credenciais de redes sociais;
- 37,1% — credenciais de *e-mail*;
- 26,8% — CPF;
- 19,3% — credenciais de banco ou cartão de crédito;
- 16,0% — credenciais de serviços de compra *on-line*;
- 14,9% — credenciais de serviços de *streaming*, como Netflix ou Spotify;
- 12,9% — outros.

Fique atento

No aplicativo de envio e recepção de mensagens mais popular no Brasil, o WhatsApp, as ações de punições podem ser feitas tanto em conversas individuais como em grupos. Em casos de crimes envolvendo conversas divulgadas em grupos, todos os usuários de um grupo poderão ser considerados responsáveis pelo conteúdo que outras pessoas enviam.

3 Princípios de investigação de crimes digitais

O grande volume de transações e acessos à Internet tem provocado um aumento significativo nos crimes digitais. Os usuários, apesar da sua desenvoltura para utilizar a Internet e navegar nas redes, ainda estão muito despreparados para reconhecer possíveis tentativas de fraudes e crimes digitais, sofrendo golpes que acabam gerando diversos prejuízos.

Muitos usuários não sabem de seus direitos e acabam ficando calados perante os crimes praticados. Apesar de existir uma percepção que os crimes digitais não são punidos, existem leis específicas para julgar esse tipo de crime. Além disso, existe um novo modelo de relacionamento entre países que cooperam com informações, as quais permitem a análise de casos que ultrapassam as fronteiras e as leis locais.

Localizar e identificar um criminoso digital é muito desafiador. Em crimes fora da rede, muitos criminosos são identificados por suas digitais, testemunhas ou evidências deixadas na cena do crime. No mundo digital, a busca por esses dados é feita em um enorme repositório de dados, por meio do endereço de IP do usuário da rede, podendo inclusive ter restrições de dados quanto ao conteúdo analisado.

Outro ponto em constante evolução são os julgamentos relacionados a crimes de injúria, difamação e calúnia, que ocorrem em grande volume nas redes sociais. Observamos uma evolução judiciária em relação a esses julgamentos, objetivando que os usuários examinem os conteúdos postados e evitem comentários indevidos em suas redes sociais. Esse tipo de julgamento somente acontecerá se a vítima acionar os órgãos competentes, realizando boletins de ocorrência e dando continuidade às ações judiciais. A melhor maneira de combater os crimes digitais é aplicar medidas similares ao sistema penal tradicional.

Em casos de crimes como roubo de dados, fraudes, pedofilia, entre outros, o processo de investigação não é uma tarefa fácil. Para chegar aos criminosos, é necessário descobrir muitas camadas de protocolo, quando estes são rastreáveis. Mesmo após a descoberta dos protocolos, são necessárias muitas autorizações para poder acioná-los judicialmente.

Saiba mais

O sistema judiciário brasileiro tem evoluído em relação ao julgamento de crimes cibernéticos, com a aprovação do novo Marco Civil da Internet (MCI) brasileira, sancionado em 23 de abril de 2014, pela Lei nº. 12.965, de 23 de abril de 2014, que regula o uso da Internet no Brasil, definindo direitos e deveres.

Outra lei brasileira específica para crimes digitais, Lei nº. 12.737, de 30 de novembro de 2012, é também conhecida como a **Lei Carolina Dieckmann**. A lei leva esse nome porque foi aprovada logo após o vazamento de fotos da atriz.

Conforme o art. 154-A da Lei Carolina Dieckmann (BRASIL, 2012, documento *on-line*):

> Art. 154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
> Pena — detenção, de 3 (três) meses a 1 (um) ano, e multa.

Mesmo o crime ocorrendo na *web* e caracterizado como crimes digitais poderá ser enquadrado em qualquer outra lei do Código Penal brasileiro, desde que o contexto do crime se aplique ao artigo da lei. Isso ocorre, por exemplo, em casos de calúnia e difamação. Uma barreira em todo esse processo é o enquadramento do ordenamento jurídico, considerando o sistema judiciário brasileiro, pois o local que ocorreu o crime nem sempre será o local do seu julgamento.

Grandes instituições financeiras têm impulsionado o governo para aprovação de leis contra crimes digitais. Esse interesse está embasado nos imensos prejuízos financeiros sofridos por fraudes que acontecem via rede. Uma reportagem do portal G1 cita que (ROHR, 2016, documento *on-line*):

> A Federação Brasileira dos Bancos (Febraban) afirma que instituições financeiras perderam R$ 1,8 bilhão com fraudes em 2015. Em 2011 (antes da aprovação da lei), a cifra era de R$ 1,5 bilhão. Embora a cifra não tenha crescido muito (ou nada, se for considerada a inflação), é difícil dizer se a "estagnação" dos prejuízos se deve à lei ou aos investimentos milionários dos próprios bancos em segurança.

O Quadro 1 apresenta os principais crimes digitais e suas respectivas tipificações.

Quadro 1. Alguns tipos de crimes digitais e leis utilizadas para o julgamento desses crimes

Crime	Tipificação em Lei
Furto eletrônico e estelionato (fraudes bancárias)	Arts. 155 e 171 do Código Penal — Decreto-Lei nº. 2.848, de 7 de dezembro de 1940 e alterações
Invasão de dispositivo informático e furto de dados	Art. 154-A do Código Penal
Falsificação e supressão de dados	Arts. 155, 297, 298, 299, 313-A e 313-B do Código Penal
Armazenamento: produção; troca, publicação de vídeos e imagens contendo pornografia infantil	Arts. 241 e 241-A do Estatuto da Criança ou do Adolescente (ECA) — Lei nº. 8.069, de 13 de julho de 1990
Assédio e aliciamento de crianças	Art. 241-D do ECA
Cyberbulling (veiculação de ofensas em *blogs* e comunidades virtuais)	Arts. 138, 139, 140 do Código Penal
Incitação e apologia ao crime	Arts. 286 e 287 do Código Penal
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	Art. 20 da Lei nº. 7.716, de 5 de janeiro de 1989
Crimes contra a propriedade intelectual artística e de programa de computador	Art.184 do Código Penal e Lei nº. 9.609, de 19 de fevereiro de 1998

Referências

BRASIL. Justiça Federal. Tribunal Regional Federal da 3ª. Região. Escola de Magistrados da Justiça Federal da 3ª. Região. *Investigação e prova nos crimes cibernéticos*. São Paulo: EMAG, 2017. 352 p. (Cadernos de estudos, 1). Disponível em: https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 28 mar. 2020.

BRASIL. *Lei Nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília: Casa Civil da Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 28 mar. 2020.

GOGONI, R. Deep Web e Dark Web: qual a diferença? *Tecnoblog*, Americana, 18 mar. 2019. Disponível em: https://tecnoblog.net/282436/deep-web-e-dark-web-qual-a-diferenca/. Acesso em: 28 mar. 2020.

PAVÃO, S. 1 em cada 5 brasileiros já foi vítima de roubo de identidade na internet. *dfndr blog*, San Francisco, 30 out. 2019. Disponível em: https://www.psafe.com/blog/roubo-de-identidade/. Acesso em: 28 mar. 2020.

PESQUISA sobre roubo de identidade. *PSafe*, San Francisco, maio 2019. Disponível em: https://cdn.blog.psafe.com/blog/wp-content/uploads/2019/05/Pesquisa-PSafe-sobre--Roubo-de-Identidade.pdf. Acesso em: 28 mar. 2020.

ROHR, A. Quem deve investigar e punir um crime on-line: pacotão de segurança. *G1 Tecnologia*, Rio de Janeiro, 14 abr. 2016. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/quem-deve-investigar-e-punir-um-crime-line-pacotao--de-seguranca.html. Acesso em: 28 mar. 2020.

SIRUL, E. What Is the Dark Web? *Experian*, Costa Mesa, 8 abr. 2018. Disponível em: https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/. Acesso em: 28 mar. 2020.

Leituras recomendadas

ABREU, C. N.; EISENSTEIN, E.; ESTEFENON, S. G. B. (org.). *Vivendo esse mundo digital*: impactos na saúde, na educação e nos comportamentos sociais. Porto Alegre: Artmed, 2013. 336 p.

BRASIL. *Lei Nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Casa Civil da Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 mar. 2020

BRASIL. Ministério da Ciência e Tecnologia. *Lei Nº 9.609, de 19 de fevereiro de 1998*. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Brasília: Casa Civil da Presidência da República, [1998]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 28 mar. 2020.

BRASIL. Ministério da Justiça. *Decreto-Lei Nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília: Casa Civil da Presidência da República, [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 28 mar. 2020.

BRASIL. Ministério da Justiça. *Lei Nº 7.716, de 5 de janeiro de 1989*. Define os crimes resultantes de preconceito de raça ou de cor. Brasília: Casa Civil da Presidência da República, [1989]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 28 mar. 2020.

BRASIL. Ministério Público Federal. 2ª. Câmara de Coordenação e Revisão. *Crimes cibernéticos*. Brasília: MPF, 2018. 275 p. (Coletânea de artigos, 3). Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 28 mar. 2020.

OLIVEIRA, R. Cinco tipos de crimes digitais devem dominar a internet brasileira em 2019. *Jornal Opção*, Goiânia, 29 set. 2019. https://www.jornalopcao.com.br/reportagens/cinco-tipos-de-crimes-digitais-devem-dominar-a-internet-brasileira-em-2019-212858/. Acesso em: 28 mar. 2020.

POZZEBOM, R. Quais são os crimes virtuais mais comuns? *Oficina da Net*, Santa Cruz do Sul, 30 abr. 2015. Disponível em: https://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns. Acesso em: 28 mar. 2020.

SURFACE Web vs Deep Web vs Dark Web vs Shadow Web vs Marianas Web. *Techdracula*, [*S. l.*], 22 dez. 2017. Disponível em: https://techdracula.com/surface-vs-deep-vs-dark-vs-vs-shadow-vs-marianas-web/. Acesso em: 28 mar. 2020.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Segurança em TI, crimes, conformidade e continuidade I

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Reconhecer o impacto na organização de problemas relacionados à segurança da informação.
- Diferenciar os principais termos utilizados na área de segurança da informação.
- Identificar os tipos de ameaças mais comuns à segurança da informação.

Introdução

Antigamente, se você tivesse algumas moedas de ouro, você as colocava em um saco de couro, escolhia um local e as enterrava, marcava o local e pronto, seu tesouro estava seguro. A informação é um precioso ativo da empresa. Quando ela era física, no formato de papel, ainda se conseguia colocar em uma gaveta com chave, fechar e a informação estava segura.

Hoje em dia, com a velocidade em que as informações cresceram, percebemos que seu volume não cabe mais em uma gaveta e, com o advento das melhorias no setor de tecnologia da informação (TI) elas podem e são compartilhadas das mais variadas formas.

Nesse contexto, surgiu a preocupação em como guardar esse bem, uma vez que a conectividade apresenta uma complexidade para que essa tarefa seja bem-feita, tanto para as pessoas físicas como para as empresas. Assim, os sistemas de informação adquirem enorme importância para as organizações, pois são a chave para o sucesso e sobrevivência, devendo ser seguros e protegidos.

Neste texto, você irá estudar como as situações envolvendo a segurança da informação podem afetar negativamente as organizações,

além de analisar como as tecnologias podem auxiliar no planejamento e na construção de um ambiente digital realmente seguro e confiável.

Sistemas de segurança

Os sistemas de segurança evoluíram juntamente a produção da informação pelo homem. Do ponto de vista histórico podemos verificar a existências de relatos de informação e forma para proteger essas informações, que foram passadas de geração em geração.

Veja os seguintes exemplos: o homem pré-histórico, 2000 anos antes de Cristo, se expressava na forma de pinturas em cavernas; posteriormente, para gravar a evolução, haviam os registros em hieróglifos e o papiro, no antigo Egito (3000 AC); os ábacos babilônicos (1800 AC); a produção de papel pelos chineses em 105 DC; as fotografias em 1826; o telégrafo em 1837; e o primeiro computador digital em 1943.

Perceba que, com o passar do tempo, as mudanças ficam cada vez mais curtas, e a necessidade de armazenar e proteger a informação também acompanha essa evolução. Note, ainda, que esse fluxo de informações deve ser protegido, se ele for interrompido ou capturado, pode gerar grandes impactos para pessoas, empresas ou até mesmo povos. Na vertente militar ao longo dos anos existem inúmeros exemplos de que se a informação não tem a segurança necessária e pode ser capturada por adversários e mudar os rumos de batalhas ou guerras.

Para as empresas, atualmente, é necessário que as preocupações sobre escolhas de sistemas de segurança de informações estejam contidas no planejamento estratégico, para que assim fiquem adequadas aos objetivos da empresa, ver Figura 1.

Figura 1. Sistemas de segurança.
Fonte: Alerta Security (2016a).

Para gerenciar, primeiro conhecemos, depois, analisamos, implantamos e administramos o assunto, seguindo assim uma sequência lógica. A importância disso está relacionada ao fato de que os ataques a informação têm crescido nos últimos anos, ocasionando consideráveis prejuízos, por exemplo, ataques do tipo **Denial of Service (DoS)** (negação de serviço) que ocorrem quando um site recebe um grande número de solicitações, além de sua capacidade, fazendo com que ele falhe e não disponibilize as informações aos usuários.

Uma forma de evidenciar esse conceito é utilizando o ciclo planejar, desenvolver, controlar e agir (PDCA, em inglês *plan*, *do*, *check*, *act*), encontrado na literatura da qualidade. Veja o Quadro1, que apresenta um resumo da ferramenta e dessa sequência.

Quadro 1. PDCA.

Planejar	Nesta fase a empresa deve conhecer suas estruturas e informações, realizando uma análise para que, assim, possa dimensionar os sistemas de segurança capazes de dar o suporte necessário as suas atividades com segurança e confiança. Aqui serão identificados os riscos (probabilidade de uma ameaça explorar uma vulnerabilidade) e as ameaças (situação em que alguém ou algo poderá causar danos a um ou vários usuários dentro da organização).
Desenvolver	Nesta fase a empresa realiza a implementação dos atributos de segurança necessários a manter a informação ao alcance de todos os envolvidos no processo, realizando essa implementação nos equipamentos e sistemas de acesso e execução de programas para o desenvolvimento das atividades afins na empresa, como a utilização de contramedidas (recursos de segurança adotados para reduzir os riscos).
Controlar	Nesta fase a empresa controla a utilização e acessos às informações para a verificação das boas práticas e se essas rotinas estão sendo utilizadas para o crescimento da organização.
Agir	Nesta fase a empresa realiza ações de melhorias nos processos ou correções, para que cada vez mais a segurança da informação tenha aderência aos processos da organização.

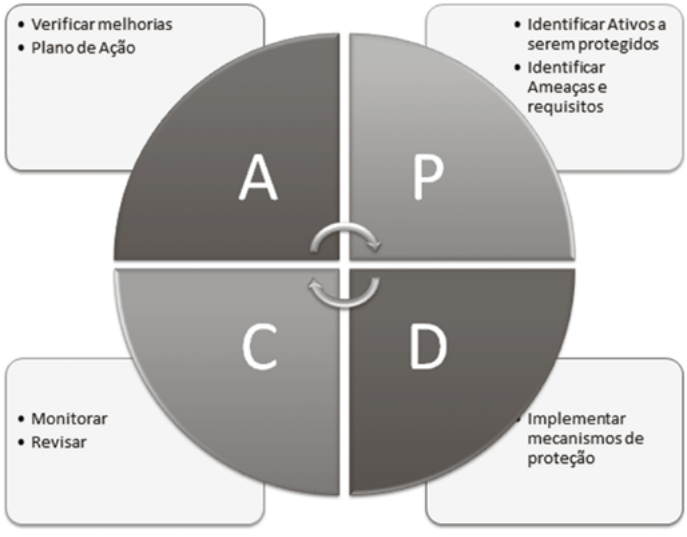

Figura 2. Ciclo PDCA.

Conhecendo a segurança da informação

A segurança da informação tem como meta a proteção da informação, seja ela impressa ou eletrônica, bem como os meios de armazenamento e utilização, por exemplo, os usuários que acessam esses equipamentos. Não basta proteger só os equipamentos se, por exemplo, os usuários liberarem informações sem as devidas permissões a pessoas fora do processo. A segurança da informação está diretamente relacionada com os riscos aos dados, aos sistemas de informação e as redes de comunicação.

Devem ser tomadas medidas para minimizar o comprometimento do vazamento das informações, por exemplo os acessos indevidos e a eliminação da informação de banco de dados. Geralmente, a segurança teve ser reforçada aos próprios funcionários das organizações, pois os maiores riscos e incidentes poder ser causados dentro da empresa.

Tratando as informações como ativos, as empresas irão preservar as informações, para isso, utilizarão os princípios da integridade, confidencialidade e disponibilidade, como você pode ver na Figura 3.

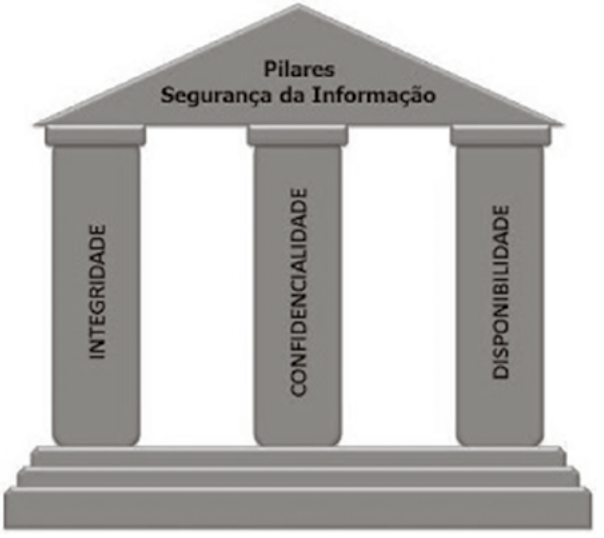

Figura 3. Pilares da segurança da informação.
Fonte: Tenca (2009).

Integridade

Integridade vem do latim *integritate*, que significa a qualidade de alguém ou algo de ser íntegro, de conduta reta, pessoa de honra, ética, educada, cuja natureza de ação nos dá uma imagem de inocência, pureza ou castidade, o que é íntegro, é justo e perfeito. Em segurança da informação, integridade significa ter a disponibilidade de informações confiáveis, corretas e dispostas em formato compatível com o de utilização.

Nesse pilar será garantido o princípio de que a informação não foi alterada de forma não autorizada, ficando, portanto, íntegra. Sendo assim, a organização terá a confiança de que suas informações não foram alteradas de maneira não autorizada ou indevida. A utilização da informação íntegra permitirá que a organização adquira conhecimento empresarial baseado na perfeita comunicação entre receptor e emissor. Se em algum momento houver uma alteração não autorizada, haverá um dano a integridade, e essa informação vai prejudicar as tomadas de decisões, ocasionando perdas para a empresa.

Dos vários aspectos que podem caracterizar a perda da integridade, dois são mais citados: as alterações do conteúdo dos documentos, quando alguém

realiza inserções, substituições ou exclusão de conteúdo ou parte dele; e as alterações nos elementos que oferecem suporte à informação, ou seja, quando há alterações na estrutura física e lógica (dados e rede) em que a informação está armazenada.

Proteger a integridade é proteger a informação, tanto nos agentes da comunicação como nos equipamentos de armazenagem, buscando assegurar o acesso correto dos sistemas e pessoas para visualizações das informações, realizar alterações autorizadas e somente utilizar as informações em prol do desenvolvimento de conhecimento empresarial aliado aos objetivos da empresa.

Confidencialidade

Confidencialidade é a qualidade daquilo que é confidencial (que se diz ou que se faz com confiança e com segurança recíproca entre dois ou mais indivíduos). Para a segurança da informação, confidencialidade é a propriedade da informação que não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização. Em outras palavras, confidencialidade é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

Nesse pilar, o grande objetivo é garantir que somente os sistemas e as pessoas que devem acessar a informação o façam, ou seja, a confidencialidade garante que a informação será utilizada somente por pessoas autorizadas e que têm acesso a ela.

Na empresa, uma ou várias pessoas necessitam, por exemplo, de uma determinada informação para realizar um processo ou fazer algum planejamento, mas essa informação não é necessária para as demais. Um claro exemplo é o custo de aquisição de uma determinada mercadoria que será posta à venda, essa informação é fundamental para o comprador adquirir e para o gestor determinar o preço de venda, mas não é importante para o segurança da empresa ou para o técnico em TI que realiza atividades de atualização do site da empresa.

Obter a confidencialidade significa dizer que o processo de comunicação da informação tem a segurança de que o que foi escrito ou dito por alguém, será recebido, lido ou escutado por quem tiver autorização. A perda de confidencialidade significa perda de segredo e pode ocasionar grandes danos em uma organização. Imagine que um produto a ser lançado é descoberto por um concorrente, ele pode melhorar algum processo e lançar o produto antes da empresa que criou o produto inicialmente, ocasionando, com isso, perdas financeiras em tempo e matérias-primas utilizadas.

Fique atento

A proteção à confidencialidade atualmente é um dos mais complexos desafios organizacionais, pois tem que garantir desde a emissão até a recepção dessa informação, passando pelos agentes e mecanismos utilizados pela empresa no processo.

Uma das formas que as organizações utilizam é a criação de níveis de confidencialidade para as informações que circulam na empresa, por exemplo, ter informações de acesso a todos, informações de acesso a setores e informações de acesso somente da direção da empresa. Dessa forma, quanto maior for o grau de confidencialidade, maior será o nível de segurança necessário para a proteção da informação. Chamamos esse processo de categorizar a informação quanto ao grau de sigilo que ela contém.

Grau de sigilo é uma graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem permissões de acesso à informação. Em geral, no mercado, os graus de sigilo aparecem da seguinte forma: confidencial, restrito, sigiloso e público.

Disponibilidade

O conceito de **disponibilidade** é utilizado em diversas áreas e esferas para fazer referência à possibilidade de que algo, um produto ou serviço, esteja disponível de ser realizado, encontrado ou utilizado. Para a segurança da informação, significa que a informação deve ficar disponível ao uso para quem tem autorização.

Neste pilar, devem ser garantidos os fundamentos de que a informação tem que estar disponível no momento em que se precisa dela. Sendo assim, os recursos tecnológicos utilizados para o acesso e armazenamento devem estar em bom funcionamento e, em caso de incidentes, serem recuperados rapidamente. Assim, o usuário ou o grupo de usuários que necessita da informação terá a garantia de a obter na hora em que precisar para seu trabalho.

A informação adquire permissões à utilização no tempo certo, alcance de todos os envolvidos e acesso quando necessário.

A disponibilidade passa por um bom planejamento em infraestruturas, permitindo a continuidade dos negócios sem prejuízos ao alcance dos objetivos organizacionais. Por exemplo, devem ser garantidos os acessos a informações confidenciais em reuniões de planejamento. Uma empresa não pode parar se

o banco de dados não puder ser acessado na realização dessa reunião ou se as informações foram perdidas por um incêndio nas instalações dos equipamentos de redes.

Partindo desse princípio, a disponibilidade deve ser protegida por meio das várias formas de proteção, como cuidados nas configurações para o trânsito das informações nas comunicações empresariais e cópias de segurança (Backups) nos dados armazenados.

Mecanismos de segurança são medidas que visam controlar o acesso às informações de forma física e lógica. Enquanto os controles físicos limitam o contato direto que um usuário pode ter com a informação e toda a estrutura que a envolve, os controles lógicos trabalham pela integridade da informação de modo que ela não seja acessada e manipulada. Alguns exemplos de mecanismos de segurança são (ALERTA SECURITY, 2016b):

- **Criptografia:** um conhecido meio de converter os dados em um formato que seja impossível decifrá-lo. Imagine que para assegurar que os dados, em idioma português, não sejam compreendidos por meros falantes da língua, as informações sejam convertidas para o hebraico. O raciocínio é muito similar a isso, porém, criptografar é impedir completamente a interpretação das informações, e elas só voltam ao estado inteligível quando uma chave (senha) for inserida.
- **Assinatura digital:** com a assinatura digital é garantida a integridade dos dados por meio de criptografia, ou seja, seu acesso pode ser irrestrito e seu conteúdo não pode ser modificado.
- **Certificação:** uma certificação é como um atestado de autenticidade de um arquivo, uma garantia de que o mesmo é válido.
- ***Honeypot*:** trata-se de um software que age como um antivírus em tempo real, cuja função é proteger os dados de invasores, aplicações maliciosas e estranhas ao sistema. A diferença é que, em vez de mantê-lo em quarentena, por exemplo, o *honeyspot* ludibria esse invasor, fazendo-o acreditar que está tendo acesso real às informações.

Crimes em informática

Os crimes em informática estão crescendo muito, tanto pelo desconhecimento como pelo aumento de usuários na rede. As informações são preciosas para seu autor seja ele uma pessoa física ou uma organização que necessita de suas informações para planejamentos ou para rodar seus processos diariamente.

Há muito tempo, as organizações procuram manter seus segredos industriais fora do alcance de curiosos ou concorrentes. Um caso clássico é a fórmula do refrigerante de cola mais famoso do mundo, a Coca-Cola. No âmbito da TI, um crime muito presente nos dias de hoje, chama-se pirataria de *software*.

Figura 4. Pirataria.
Fonte: Universidade Federal do Sul e Sudeste do Pará (2016).

No Quadro 2, você verá as modalidades desse crime, citados na Lei nº 9.609/1998 (BRASIL, 1998), que estabelece que a violação de direitos autorais de programas de computador é crime, punível com pena de detenção de 6 meses a 4 anos e multa, além de ser passível de ação cível indenizatória.

Quadro 2. Crimes de informática.

Crimes de falsificação	Trata-se de cópia de um software protegido por direitos autorais que é imitado em sua embalagem, etiqueta e demais informações, com visual muito próximo ao original para sua comercialização.
CDROM pirata	Também é um caso de falsificação, só que neste caso o usuário já sabe que está adquirindo uma cópia ilegal do que está procurando, por exemplo, um programa, um filme ou uma música, é encontrado normalmente em pontos de comércio popular, feito em uma mídia regravável, com valor bem abaixo do normal. Em uma única mídia é possível encontrar uma coletânea de mais de um original, por exemplo, todos os lançamentos de um músico.
Revendas de *hardware*	Acontece quando uma empresa ou pessoa vende um computador, seja em uma loja física ou virtual e entrega esse hardware com algum programa instalado pirata ou afirmando ser original, mas sem oferecer ao usuário a licença original ou a documentação técnica. Por exemplo, você compra um notebook já com o programa operacional instalado e não se preocupa em verificar se esse programa foi devidamente licenciado.
Pirataria individual	Ocorre quando uma pessoa, por amizade ou por não entender a gravidade do ato, oferta programas que comprou a colegas ou amigos, ela tem a licença de uso individual, mas realizando esse ato de compartilhar acaba por criar um problema grande não percebendo a gravidade e dimensão que isso pode ocasionar.
Pirataria corporativa	Parte do mesmo princípio da pirataria individual, ocorrendo em progressão geométrica. Imagine em uma empresa, ela compra licença de uso para um computador e instala nos outros 199 que possui. Nesse tipo de pirataria estão concentradas as maiores perdas do setor de software, pois são muitos hardwares funcionando com licenças copiadas. De fato, não são todas as organizações que cometem esse delito, há muitas que tem um rígido controle sobre o uso e adquirem corretamente as licenças para uso de programas.
Pirataria cliente/ servidor	Geralmente ocorre quando uma empresa entra em rede, ou seja, deixa de operar com estações separadas e utiliza um servidor com estações ligadas em rede. Nesse processo pode que ter, mesmo sem saber (quando faz o serviço com terceiros), instaladas cópias piratas ou acessos ilegais a programas compartilhados com um limite maior do que a licença permite, sendo essa prática um crime.
Pirataria *on-line*	Atualmente não há como ficar desconectado, seja em casa ou nos ambientes coorporativos. Com esse advento, a pirataria on-line vem crescendo na mesma proporção, os software são transferidos e instalados ilegalmente e anonimamente.

Fonte: Brasil (1998).

Fique atento

Software são obras intelectuais, e não um produto. Quando adquirimos um software, estamos adquirindo a licença de uso, portanto, quem compra uma cópia pirata está tão sujeito a punições quanto quem comercializa.

Não devemos discutir o valor de cada software, mas sim procurar realizar nossas ações baseadas na ética e na moral, pois esse tipo de crime é muito cultural e deve ser combatido.

Para as empresas, cabe ao empresário responder por qualquer irregularidade que ocorra dentro de sua organização. Mesmo que ele não tenha incentivado a instalação de algum software, é responsável pelo monitoramento de suas estações de trabalho e de praticar ações preventivas e orientações a respeito do tema.

O caminho a percorrer é longo, por tratar-se de um problema cultural, por isso, as empresas estão cada vez mais criando e executando políticas bem claras sobre o tema, com objetivo de minimizar os prejuízos que podem aparecer com esse tipo de crime. Não basta só o amparo legal, é preciso haver uma conscientização coletiva para minimizar os impactos negativos que a pirataria causa.

Lembre-se que qualquer pessoa envolvida com a prática ilícita (pirataria) está sujeita a punições que variam de 6 meses a 2 anos de detenção, além do pagamento de indenizações.

Os sistemas de informação estão sempre sujeitos a sofrerem ameaças, tanto internamente como externamente. Essas tentativas podem ser, como vimos, intencionais, mas também podem não ser intencionais, como uma codificação errada de uma funcionalidade do software por um entendimento incorreto do profissional (programador). É necessário separar esses dois tipos de ameaças.

Saiba mais

O presidente do Fórum Nacional Contra a Pirataria e Ilegalidade (FCNP), Edson Vismona, informou que, em 2015, o Brasil teve perdas da ordem de R$ 115,603 bilhões em **piratarias**, **contrabando** e **sonegações**. O montante contabiliza perdas de setores como vestuário, cigarros e TV por assinatura. Segundo ele "[...] acredito que pode ter sido muito mais, já que não há setores nessa conta, como o automobilístico, por exemplo." (ESTADÃO CONTEÚDO, 2016).

Insegurança na internet

A rede de computadores veio para o auxiliar a disseminação da informação e o acesso mais democrático delas pelas pessoas e empresas que antes não podiam ter acesso. Assim, além dos benefícios vieram também os malefícios da modernidade.

Dentre os fatores que contribuem para a insegurança no acesso, aparece a falta de conhecimento, por parte da maioria dos usuários; o anonimato, que protege os maus usuários; os criminosos; e a pouca disseminação e a própria falta de interesse na segurança por parte do usuário, que acaba por terceirizar a preocupação com segurança a seu provedor de internet. Você deve lembrar que o assunto segurança é de responsabilidade de todos, por exemplo, quando você dirige um carro na preferencial, entende que tem a preferência e, caso ocorra uma colisão, você estará certo e a outra pessoa errada, isso é fato, mas o inconivente de ficar sem carro ou um período até que seja concertado é seu.

Todos estão expostos a um inconveniente, portanto, o melhor é prevenir. Na TI, o nome do criminoso é conhecido como hackers, que são usuários que focam suas ações em praticar atos contra pessoas ou empresas com objetivos próprios e seu favor, sejam por poder ou financeiros.

São muitos os motivos que levam esses criminosos a agir, entre eles:

- **Espionagem:** podem ser militares, de estado ou em empresas industriais, podem ser contratados por concorrentes ou inimigos para roubar ou destruir os dados de outros.
- **Proveito próprio:** quando o ataque objetiva obter proveitos próprios, muitas vezes financeiros, por exemplo: transferências de numerário, resultados de concursos, uso de redes de telefonia ou dados sem os encargos.
- **Vingança:** pessoas comuns, empresas ou até mesmo outro criminoso, pode até ser realizado por um não hacker, pode ser um ex-funcionário que está descontente com a antiga empresa, ou um ex-namorado que sai de um relacionamento e quer prejudicar a outra parte.
- **Status, poder, necessidade de aceitação:** há nitidamente uma concorrência entre esses criminosos, eles querem sempre superar seus pares, sendo reconhecidos nesse submundo.
- **Aventura:** esses criminosos, em maioria, são dotados da necessidade de aventura e desafios, partindo, por exemplo, do grau de dificuldade de invadir determinado sistema, os alvos mais cobiçados são plataformas de governos e instituições de segurança mundial.

- **Maldade:** infelizmente o simples prazer de destruir faz parte do dia a dia desses criminosos, alguns deles têm o ego alto e para satisfazer esse ego cometem os crimes.

No Quadro 3, você verá os principais termos de crimes, ou ações que podem virar crime, que ocorrem na rede.

Quadro 3. Termos de crimes.

***Adware* (junção das palavras em inglês *advertisement*, "anúncio", e *software*, "programa")**	É projetado para apresentar propagandas, tem um formato de dar retorno financeiro para aqueles que desenvolvem software livre ou prestam programas gratuitos, seu mau uso pode vir a acontecer na forma de *spyware*, ou seja, que vire um espião para monitorar os hábitos dos usuários durante a execução ou navegação para direcionar as propagandas de determinados produtos ou serviços.
***Keylogger* (do inglês, "registrador do teclado")**	É um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente é ativado pós o uso por um usuário em um site de comércio eletrônico ou a internet banking, capturando assim as senhas.
***Phishing* (derivada da palavra em inglês *fishing*, que significa "pescaria")**	Trata-se de mensagens não solicitadas, passando-se por empresas conhecidas procurando induzir os usuários ao fornecimento de dados pessoais, de segurança ou financeiros. Podem ainda induzir os usuários a instalarem programas maliciosos para futuras invasões.
***Scam* ou "golpe"**	Termo usado para se referir a comunicações não solicitadas que são enviadas a um grande número de pessoas, aleatórias ou não, com objetivo de originar ganhos financeiros com ações ou delitos.
Vírus	Programa ou parte de programa perigoso ou malicioso que infecta programa ou arquivos em um computador, assim como em humanos ele pode ficar hospedado e um tempo depois ativar dando continuidade ao processo de infecção para destruir ou repassar dados a outros;
Vulnerabilidade	Pode caracterizar-se por falhas em projetos de implementação ou configuração de um sistema operacional, mesmo em sua criação, podendo, assim, originar violação da segurança nas estações de trabalho. Pode ser apresentada na forma de exploração (baseada no uso de ferramentas ou técnicas, com intuído de obter vantagens).
***Worm* (do inglês, "verme")**	É uma espécie de programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Ele se aproveita de vulnerabilidades de segurança ou falhas na configuração de softwares instalados para, posteriormente, ocasionar lesões.

Baseados nessas informações, cada vez mais as pessoas e as empresas têm que criar hábitos para melhorarem o aspecto segurança, criando padrões de proteção aos seus dados e visando à segurança de informações para garantir a integridade, a confidencialidade, a autenticidade e a disponibilidade das informações que irão gerar conhecimento.

A informação é um ativo, sendo importante a qualquer organização e, hoje, até mesmo sendo considerado o ativo de maior importância e mais crítico. Lembre-se que se a informação for adulterada, ou não estar disponível para a tomada de decisão, pode influenciar muito os resultados da organização, gerando inclusive perdas financeiras.

Em um cenário pessimista esse tipo de crime pode levar a empresa a inviabilizar a continuidade de seus negócios se for negligenciada a segurança.

Saiba mais

Os possíveis tipos de *phishing* são (SEU MICRO SEGURO, 2016):

- ***Phishing* tradicional:** esse tipo de ataque é o mais simples na hora de analisá-lo tecnicamente; normalmente está vinculado à cópia de um site conhecido pela vítima no qual é alterado o endereço para onde irão os dados inseridos.
- ***Phishing* redirecionador:** assim como o caso anterior, essa técnica é utilizada em campanhas massivas, apesar do baixo percentual de vítimas, existe uma grande quantidade de usuários afetados e, consequentemente, credenciais comprometidas.
- ***Spear phishing*:** a principal diferença desse tipo é ser direcionado à poucas pessoas ou grupos reduzidos, dessa forma, as campanhas são muito mais personalizadas e com um percentual muito maior de vítimas.
- ***Smishing SMS*:** esse tipo de *phishing* está relacionado ao uso de outro canal digital como os telefones celulares. Normalmente, os cibercriminosos se passam por instituições conhecidas e enviam uma mensagem de texto alertando à vítima que ganhou um prêmio.
- ***Vishing*:** como citado anteriormente, existe o estabelecimento de falsos centros de atendimento telefônico que realizam ligações com o objetivo de cometer uma fraude, relacionando-as com casos de *vishing*. Esse ataque, muitas vezes, está relacionado a outro, de forma que se complementem para conseguir mais credibilidade e, dessa maneira, enganar à vítima de uma forma mais simples e eficaz.

Exercícios

1. As organizações vem se modernizando à medida que as Tecnologias da Informação (TI) sofrem constantes evoluções. Dificilmente, uma empresa moderna sobrevive no mercado sem utilizar recursos tecnológicos na execução de suas tarefas. Contudo, ao mesmo tempo em que ajudam a empresa na sua gestão, as TI podem ser utilizadas por pessoas interessadas em comprometer a segurança das informações organizacionais, tendo como objetivo final o ganho de benefícios indevidos. Em relação à segurança da informação, identifique a afirmação correta.

a) A segurança da informação direciona seus esforços para ataques realizados por cibercriminosos, uma vez que eles ocasionam maiores perdas financeiras.

b) A segurança da informação está diretamente relacionada com os riscos aos dados, aos sistemas de informação e às redes.

c) As novas tecnologias de proteção a dados são, na maioria dos casos, as culpadas por problemas de segurança da informação.

d) Ações reativas não necessitam ser especificadas em um plano de gestão de riscos de TI, pois as ações preventivas são capazes de abordar todos os possíveis problemas.

e) Considerando o baixo potencial de impacto dos atuais vírus de computador, a organização pode priorizar a proteção a outras formas de ataque.

2. A segurança da informação e a segurança de redes corporativas não estão relacionadas apenas ao uso de hardwares e softwares para prevenir ou reagir a incidentes. Na verdade, toda e qualquer defesa tecnológica é importante, mas a proteção aos dados e às operações das empresas requer uma abordagem mais ampla, envolvendo desde a implementação de procedimentos e políticas de uso dos recursos tecnológicos até a garantia do cumprimento de leis e regulamentações governamentais. Nesse contexto, analise as afirmações a seguir.

I. Os maiores riscos e, consequentemente, os maiores incidentes são causados pelos próprios funcionários das organizações.

II. As ameaças à segurança da informação acontecem tanto com o uso de alta tecnologia como pelos crimes tradicionais, como o roubo de um notebook da empresa, por exemplo.

III. É importante tratar a segurança da informação como uma função isolada na organização, pois assim ela será capaz de auxiliar no alcance dos objetivos estratégicos.

Está correto o que se afirma apenas em:

a) I e II.

b) I e III.

c) II e III.

d) I, II e III.

e) Nenhuma das afirmações.

3. A área de segurança da informação utiliza diversos termos técnicos que

devem ser bem compreendidos e diferenciados pelos gestores, especialmente aqueles cuja atuação está diretamente relacionada à proteção dos dados e redes da organização. Esse conhecimento é fundamental para que as ferramentas corretas sejam empregadas em cada situação que envolva a segurança da informação. Analise os termos apresentados a seguir e relacione-os corretamente a seus conceitos.

I. Risco.
II. Ameaça.
III. Contramedida.
IV. Exploração.

( ) Uso de alguma ferramenta ou técnica com o intuito de obter vantagem de uma vulnerabilidade.
( ) Recurso de segurança adotado para reduzir riscos.
( ) Probabilidade de uma ameaça explorar uma vulnerabilidade.
( ) Situação em que alguém ou algo pode causar danos a um ou vários ativos.

Identifique a alternativa que apresenta a relação correta entre os termos e seus respectivos conceitos.

a) II, I, III, IV.
b) III, II, I, IV.
c) III, IV, I, II.
d) IV, I, III, II.
e) IV, III, I, II.

4. Os sistemas de informação estão sujeitos a sofrer diversas ameaças, ocasionadas tanto por agentes internos (funcionários) como por agentes externos, os cibercriminosos, por exemplo. Normalmente, essas ameaças tentam se aproveitar de vulnerabilidades existentes no ambiente tecnológico da organização. Uma classificação comumente encontrada na área de segurança da informação para as ameaças é relacioná-las como intencional ou não intencional, sendo esta última ainda categorizada como erro humano, riscos ambientais ou falhas nos sistemas computadorizados. Analise as afirmações a seguir e identifique aquela que apresenta corretamente um exemplo real de ameaça intencional ou não intencional.

a) dados falsos são inseridos no computador do usuário para que ele seja obrigado a negar essa alteração de arquivos.
b) o usuário abre algum anexo de e-mail infectado com vírus, espalhando essa praga por toda a rede.
c) todos os computadores da empresa são automaticamente desligados por vírus.
d) um servidor ou site recebe um número de solicitações maior do que sua capacidade de resposta, fazendo com que ele falhe.
e) um usuário exclui, deliberadamente, registros de um sistema de informação para prejudicar a execução do serviço por outros usuários.

5. Empresas de monitoramento de redes relatam que o número de ataques vem crescendo nos últimos anos, ocasionando consideráveis prejuízos, especialmente financeiros. Normalmente, os ambientes das grandes empresas e dos governos são os que mais sofrem ataques. Como a variedade de ataques é grande, a tarefa de defender o ambiente virtual é muito complexa

e nem sempre consegue obter sucesso. Um ataque do tipo DoS (Denial of Service – Negação de Serviço) ocorre quando:

a) dados falsos são inseridos no computador do usuário para que ele seja obrigado a negar essa alteração de arquivos.

b) o usuário abre algum anexo de e-mail infectado com vírus, espalhando esta praga por toda a rede.

c) todos os computadores da empresa são automaticamente desligados por vírus.

d) um servidor ou site recebe um número de solicitações maior do que sua capacidade de resposta, fazendo com que ele falhe.

e) um usuário exclui, deliberadamente, registros de um Sistema de Informação (SI) para prejudicar a execução do serviço por outros usuários.

Referências

ALERTA SECURITY. *Entenda as diferenças entre segurança da informação e segurança em TI*. São Paulo, 2016a. Disponível em: <https://www.alertasecurity.com.br/blog/168-entenda-as--diferencas-entre-seguranca-da-informacao-e-seguranca-em-ti>. Acesso em: 13 ago. 2017.

ALERTA SECURITY. *Entenda o que é segurança da informação e reduza riscos na empresa*. São Paulo, 2016b. Disponível em: <https://www.alertasecurity.com.br/blog/117-entenda-o--que-e-seguranca-da-informacao-e-reduza-riscos-na-empresa>. Acesso em: 13 ago. 2017.

BEZERRA, F. *Ciclo PDCA*: conceito e aplicação (guia geral). [S.l.]: Portal Administração, 2013-2015. Disponível em: <http://www.portal-administracao.com/2014/08/ciclo--pdca-conceito-e-aplicacao.html>. Acesso em: 13 ago. 2017.

BRASIL. *Lei nº 9.609, de 19 de fevereiro de 1998*. Brasília, DF, 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>. Acesso em: 14 ago. 2017.

DEVMEDIA. *Segurança em bancos de dados*: aplicando normas e procedimentos - Revista SQL Magazine 103. Rio de Janeiro, c2017. Disponível em: <http://www.devmedia.com.br/seguranca-em-bancos-de-dados-aplicando-normas-e-procedimentos-revista--sql-magazine-103/25669>. Acesso em: 14 set. 2017.

ESTADÃO CONTEÚDO. *Pirataria e falsificação levaram a perdas de R$ 115,6 bilhões em 2015*. [S.l.]: Brasil Econômico, 2016. Disponível em: <http://economia.ig.com.br/2016-07-01/pirataria-contrabando-sonegacao-prejuizo-2015.html>. Acesso em: 14 ago. 2017.

SEU MICRO SEGURO. *Conheça os 5 tipos mais comuns de phishing*. [S.l.], 2016. Disponível em: <https://seumicroseguro.com/2016/12/06/conheca-os-5-tipos-mais-comuns-de--phishing/>. Acesso em: 13 ago. 2017.

TENCA. *Definição da segurança da informação*. [S.l.]: Segurança da Informação, 2009. Disponível em: <http://segtenca.blogspot.com.br/2009/08/definicao-da-seguranca--da-informacao.html>. Acesso em: 14 set. 2017.

Leituras recomendadas

BRASIL. Departamento de Polícia Rodoviária Federal. *Dia nacional de combate à pirataria*. Brasília, DF, c2017. Disponível em: <https://www.prf.gov.br/portal/noticias/nacionais/dia-nacional-de-combate-a-pirataria>. Acesso em: 13 ago. 2017.

CARNEIRO, A. *Auditoria e controle de sistemas de informação*. Rio de Janeiro: FCA, 2009.

LYRA, M. R. *Segurança e auditoria de sistema de informação*. Rio de Janeiro: Ciência Moderna, 2008.

NONATO, A. A. M. *Os crimes digitais em nosso cotidiano*. [S.l.]: Âmbito Jurídico, c1998-2017. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=8890>. Acesso em: 13 ago. 2017.

SANTA CATARINA. Secretaria de Estado do Desenvolvimento Econômico Sustentável. Conselho Estadual de Combate à Pirataria. *Perdas com contrabando chegam a 115 bi, estima fórum antipirataria*. Florianópolis: CECOP, c2017. Disponível em: <http://www.sds.sc.gov.br/cecop/index.php/noticias/255-perdas-com-contrabando-chegam-a-115-bi-estima-forum-antipirataria>. Acesso em: 13 ago. 2017.

UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ. *Instalação de software pirata é crime!* Marabá: CTIC, 2016. Disponível em: <https://ctic.unifesspa.edu.br/index.php/ultimas-noticias/234-instalacao-de-software-pirata-e-crime>. Acesso em: 14 set. 2017.

Segurança em TI, crimes, conformidade e continuidade II

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Diferenciar os conceitos de crime, fraude e violações no contexto da segurança da informação.
- Distinguir entre controle de acesso por autorização e controle por autenticação.
- Relacionar os processos de autoria com a continuidade dos negócios da organização.

Introdução

Atualmente, quanto maior for à utilização da tecnologia no ambiente empresarial, maior deve ser a preocupação com a segurança. Todo dia pessoas levantam para trabalhar honestamente, mas uma parcela da população nem dorme, arquitetando alguma forma de levar vantagem sobre outra, seja monetária ou de poder.

O caminho da evolução tecnológica não tem volta, pois veio para auxiliar pessoas e empresas há terem um dia a dia melhor, com mais informações e um maior alcance a públicos que antes eram distantes. Hoje, você pode se relacionar com pessoas que antes nem sonhava que existiam, e as empresas podem comprar e vender seus produtos e serviços a clientes que antigamente era quase que impossível em razão do altos custos.

Qual a grande chaga do momento? A segurança. Ela tem que ser construída para evitar crimes, fraudes e violações. Sejam eles quais forem somente será possível minimizar os efeitos noviços se trabalharmos em conjunto.

Neste texto, você verá a importância das auditorias para consolidar a segurança da informação dentro das organizações e os conceitos desses delitos, presentes no nosso dia a dia. Esse é o primeiro passo, conhecer para combater.

Crimes, fraude e violações

Para um melhor entendimento de crime, primeiramente segue o conceito de lei: Segundo o art. 1° da Lei de Introdução do Código Penal – Decreto Lei nº 2.848 de 7 de dezembro de 1940: "[...] considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativamente ou cumulativamente com a pena de multa; contravenção, a infração penal que a lei comina isoladamente, penas de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente." (BRASIL, 1940).

Para a área de tecnologia da informação (TI) os crimes começam na forma eletrônica e, quando concretizados, descobertos, investigados e condenados, vão incidir nos mesmos artigos das leis cíveis que regem os cidadãos brasileiros.

Você, em seus estudos, já deve ter percebido que os crimes estão em uma crescente, pelas condições apresentadas em nosso país ontem e hoje, com uma velocidade maior. Estamos vendo o crescimento dos crimes em informática, em razão da velocidade com qual as pessoas e empresas entram na rede. Sem o devido tempo de primeiramente aprenderem os conceitos básicos de segurança, as pessoas e empresas ficam expostas a todo o tipo de crime cometido nessa seara, como as piratarias e falsificações.

Você deve lembrar que já há uma legislação específica (Lei nº 9.609/1998 que estabelece que a violação de direitos autorais de programas de computador é crime, punível com pena de detenção de 6 meses a 4 anos e multa, além de ser passível de ação cível indenizatória) para esse tipo de crime, mas ainda há um longo caminho a ser percorrido para a efetiva ação de punição aos criminosos.

A fraude tem o significado de ser uma atividade, ação ou atitude que, sendo desonesta, tem a finalidade de intrujar, prejudicar ou ludibriar alguém, sendo passível de ser punida legalmente. Também é definida como a ação de forjar algo, por exemplo, documentos, marcas ou bens, para comercializar no lugar dos produtos originais.

As fraudes também podem ocorrer no caso de mercadorias contrabandeadas de outro país e que entram ilegalmente no nosso país, sem o devido pagamento dos impostos locais.

Assim como os crimes, as fraudes ganham um campo fértil na rede de computadores, por desinformação, os usuários acabam por se descuidar e caírem em golpes apresentados na internet, por exemplo, a compra de produtos ou serviços que são pagos e não são enviados ao comprador.

A violação tem o significado de violar, desrespeitar algo no direito, por exemplo, é um crime contra a mulher o ato de "violar" o ser, é uma forma de transgressão as leis a ordem e a outras pessoas.

Na área de TI, essas violações geralmente são em dados sem a permissão, a violação de sistemas, entre outras formas.

Portanto, em alguns casos essas três definições se misturam com um único objetivo: obter vantagens sobre alguém ou alguma empresa, pode ser um caso de um acesso indevido. Isso pode ocorrer por uma violação de senhas, que vai acarretar em um crime financeiro, por exemplo. Enfim, são muitos os exemplos que temos atualmente, visto que não há mais como estar fora do mundo digital.

Você deve lembrar que a primeira linha de defesa para esses crimes é o conhecimento, com o conhecimento da importância da segurança, serão traçadas as políticas de segurança. Em casa você, por exemplo, sabe que se acessar algum site desconhecido poderá de alguma forma infectar sua estação de trabalho de forma que um elemento possa se apropriar de seus dados pessoais com objetivos diversos. Em uma empresa esse cuidado fica mais crítico, pois uma invasão pode ocasionar as mesmas perdas, só que em grande proporção.

Veja nos Quadros 1, 2 e 3 um resumo das principais categorias de crimes, fraudes e violações, correlacionadas com a TI.

Quadro 1. Categorias de crimes.

Crimes violentos	São as formas mais violentas contra pessoas e empresas, aquelas ocorrências classificadas como homicídio, homicídio tentado, estupro, roubo e roubo à mão armada, segundo a caracterização determinada pelo Código Penal Brasileiro (BRASIL, 1940), nos delitos praticados pela rede de computadores ainda é raro esse crime puro, ele pode originar-se de ações na rede, mas não o ato de fato.
Crimes não violentos	Tratam-se normalmente de ações ilícitas sem fins de lesão corporal ao "não bem material", ou seja, qualquer crime que não resulte em dano físico a vítima (pelo menos diretamente). Nessa categoria encontramos a maioria dos delitos relacionadas à área de TI.

Quadro 2. Categorias de fraudes.

Fraude efetiva ou deliberada	Ocorre quando um fraudador ou um grupo de fraudadores investe contra um estabelecimento comercial físico ou eletrônico, utilizando dados roubados para efetuar transações comerciais que não serão pagas, ocasionando aos lojistas perdas financeiras.
Autofraude	Neste tipo de fraude não há o roubo ou captura dos dados de pessoas, a própria pessoa efetua a compra, recebe os produtos ou serviços e depois entra em contato com a operadora de cartão de crédito não reconhecendo a transação, com o propósito de não efetuar o pagamento da transação. É uma situação difícil de ser detectada no começo, pois os dados são de fato do usuário.
Fraude amigável	Ocorre quando um conhecido, ou até mesmo um familiar se apropria dos dados de uma pessoa para realizar uma compra sem o consentimento dela, por exemplo, utilizando o cartão de crédito para compras pela rede de computadores ocasionando dano ao fornecedor das mercadorias ou serviços, também é um tipo de fraude difícil de detectar em um primeiro momento.
Fraude ocupacional	Ocorre quando colaboradores de uma organização utilizam os recursos disponíveis para seu trabalho em proveito próprio, por exemplo, a utilização da internet corporativa para pesquisas pessoais, a impressão de material pessoal em impressoras da organização, uso de telefone para ligações pessoais, enfim uma série de atos em horários não permitidos com a utilização de recursos corporativos para fins pessoais.
Apropriação indevida	Essa fraude ocorre quando um colaborador desvia ou utiliza indevidamente ativos e recursos da empresa, são exemplos os furtos, a manipulação de despesas ou de estoque (inventário) com objetivo de proveito próprio.
Corrupção/ suborno	Ocorre quando se utiliza a influência ou poder para se obter uma vantagem (para o autor e/ou em terceiros) contrária ao dever para com a entidade empregadora ou ao direito da contraparte. Podemos identificá-la por meio do suborno, conflito de interesses, extorsão econômica e desconto impróprio, ocorre dentro das organizações e entre pessoas ou organizações e o governo.
Demonstrações fraudulentas	Esse tipo de fraude é muito comum na área de TI, e é o meio de como fazer. As fraudes ocorrem com a inclusão de informações não verdadeiras em relatórios de demonstrações financeiras ou não financeiras, com objetivo de ocultar as informações verdadeiras. É também chamada de "maquiagem" ou como recentemente conhecemos no caso do governo "pedaladas", tendo o objetivo claro de induzir o leitor dos relatórios ao erro e com isso a tomada de decisão errônea.

Quadro 3. Categorias de violações.

Violações para roubo de identidade	Ocorrem quando um criminoso invade a segurança de pessoas ou empresas com o objetivo de capturar dados pessoais ou corporativos para, em um segundo momento, utilizar esses dados para obter vantagens para si. Esse tipo de violação é a mais comum e que exige cada vez mais investimentos na área de segurança de TI das organizações para ser minimizado.
Violações contra os direitos autorais	A violação contra os direitos autorais ocorre quando uma pessoa ou empresa captura obras de um autor, sem respeitar os seus direitos de autoria. Há inúmeros exemplos desse tipo de violação, muito comum com obras literárias, musicais ou projetos de produtos ou processos industriais.
Violações contra a liberdade de expressão	Todos têm, de acordo com a Constituição de nosso país (BRASIL, 1988), o direito a liberdade de expressão, mas esse princípio, muitas vezes, não é respeitado, principalmente com o advento da modernidade que trouxe a facilidade da liberdade de expressão e, com isso também a facilidade para a violação desse direito. Um exemplo é a utilização da rede para não respeitar e atacar a liberdade, como em casos de barrar ou bloquear a informação por parte da imprensa ao público em geral. Ocorre também dentro das organizações, quando a informação que deveria ser de conhecimento de todos, acaba por não ser.

Link

Roubo de identidade foi o principal tipo de violação de dados em 2016, em que 1.792 violações de dados comprometeram quase 1,4 bilhão de registros de dados no mundo inteiro, o que gerou um aumento de 86% em comparação a 2015. Esse número correspondeu a 59% de todas as violações de dados. Além disso, 52% das violações de dados em 2016 não tiveram o número de registros comprometidos revelado, quando reportados. Se quiser se aprofundar mais sobre esse tema, acesse o link ou código a seguir (INSIDE, 2017).

https://goo.gl/jmt7Nq

Auditoria nas organizações

O termo auditar significa realizar um exame sistemático das atividades desenvolvidas em uma determinada empresa ou setor, que vai ter como objetivo averiguar se elas estão de acordo com as disposições legais ou planejadas/estabelecidas previamente, se foram implementadas com eficácia e eficiência e se estão adequadas aos normativos existentes, tanto internos como externos, por exemplo, atendendo a legislações como a do meio ambiente.

Antigamente, utilizava-se o termo inspetoria, que tinha um aspecto mais punitivo. Atualmente, o termo mais usado é auditoria, que faz o exame e auxilia as organizações a melhorarem seus processos atendendo assim a todos os *stakehorders* (público estratégico).

As auditorias podem ser internas ou externas, dependendo do contexto e da complexidade da atividade em que a empresa atua. Geralmente, no mercado financeiro são realizadas as duas versões, internas para melhorar os processos e externas para averiguar se os dados disponibilizados para o mercado estão de fato corretos, sempre com o objetivo de atestar e melhorar os processos.

Veja, na Figura 1, em um exemplo de organograma empresarial, qual a posição das auditorias.

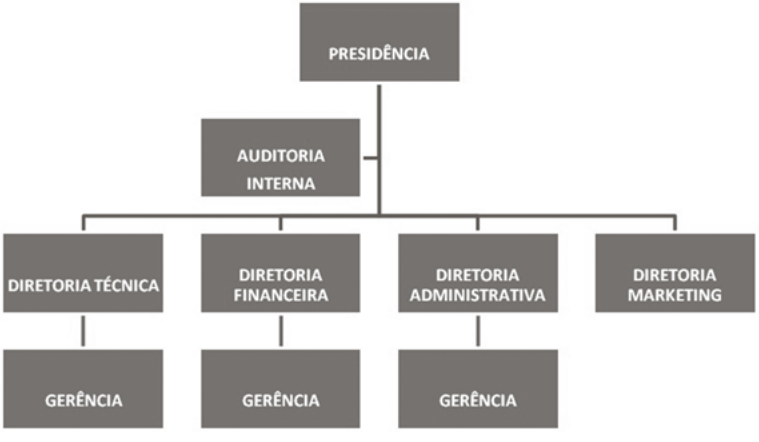

Figura 1. Organograma empresarial.
Fonte: Portal de Auditoria (2016).

As auditorias internas ou externas não ficam no eixo central das empresas, mas sim atuando diretamente reportadas a alta direção, com o objetivo de verificar e melhorar os processos de todas as áreas da organização.

Para nosso contexto, vamos ver a auditoria de sistemas, que tem importância fundamental para as organizações, pois cada vez mais as empresas investem muito em sistemas computadorizados e precisam garantir que esses recursos sejam utilizados com segurança e que tenham qualidade nas informações geradas, garantido a correta tomada de decisão.

Essa área ainda está em desenvolvimento e faltam profissionais habilitados, pois as áreas de conhecimento em sistemas são vastas, ocasionando uma grande necessidade de tempo para formar bons profissionais. Outro fator é a falta de cultura dentro da organização, que completa o quadro de dificuldades enfrentadas. Isso não diminui a necessidade da realização das auditorias, pois com a realização as organizações fortalecem as técnicas de segurança, criam metodologias de processos e melhorias nas suas performances como um todo.

O profissional de TI que migrar para essa área, deve ser independente, formado em cursos de auditoria de computação e conhecer o ambiente em que fará suas atribuições. Ele terá uma grande preocupação com a qualidade dos processos auditados, auxiliando a empresa a obter uma melhor segurança e confiança no conhecimento gerado pelos dados e informações.

O processo de auditoria é um processo todo planejado, com padrões a serem seguidos e obedecidos, principalmente na ética do profissional que irá executar o trabalho. Lembre-se que uma auditoria bem definida e executada deve ser realizada por um profissional isento e imparcial em suas análises e conclusões. O Quadro 4 apresenta um exemplo de organização do trabalho de um auditor.

Quadro 4. Organização do trabalho de auditoria.

Planejamento	Nesta fase o profissional vai conhecer o ambiente a ser auditado, levantar todos os dados pertinentes ao trabalho, identificar os pontos críticos a serem analisados, traçar os objetivos e critérios que irá utilizar, verificar a análise de risco das atividades e definir os pontos de controle, nunca esquecendo os prazos a serem cumpridos nem das ferramentas tecnológicas que irá utilizar.
Definição da equipe	Normalmente o auditor irá utilizar uma equipe multifuncional, para tal deve conhecer o perfil e o histórico desses profissionais, suas experiências profissionais e sua ética. Após, deve estabelecer programas e cronogramas de trabalho para executar, revisar e avaliar a produção da equipe para o alcance dos objetivos traçados no planejamento.
Documentação de trabalho	Sem padronização não há auditoria, o trabalho tem que ser documentado e registrado, assim irá conter relatórios, manuais e outros que servirão de fonte para a determinação dos pontos positivos e pontos a serem melhorados dentro do processo analisado.
Apresentação dos resultados	É a parte que o auditor ou a equipe de auditores apresentam os resultados a alta direção da empresa, não só apontando os erros, mas também fazendo sugestões e recomendações de melhorias. Todo conteúdo da auditoria deve ser bem explicado e amparado nas normas e controles da empresa, assim como comparações de boas práticas realizadas pelo mercado, por exemplo, se em outra empresa do ramo, os profissionais estão com uma melhor garantia de segurança de dados.

As auditorias de sistemas irão cuidar do processamento eletrônico de dados, com isso irão atuar no hardware, software e teleprocessamento das informações. Atuam fortemente nos sistemas de informação (conjunto de recursos humanos, materiais, tecnológicos e financeiros que são utilizados para o transporte de dados, informações e conhecimento dentro de uma empresa) utilizados pelas organizações, afinal a detecção de problemas de segurança da informação deve ser realizada com a maior brevidade possível, facilitando para a empresa a atuação de combate ao problema, a melhoria dos processos e a redução de custos com possíveis danos causados pelo vazamento ou má utilização das informações.

Outro termo bastante utilizado em segurança é o "controle interno", que tem o conceito de atuar na verificação e validação dos parâmetros dos sistemas de informação, sendo: a confiança dos dados apresentados, sua segurança física e lógica, a confidencialidade desses dados, o atendimento as legislações vigentes, a obediência as políticas internas da organização e a utilização dessas informações com eficiência e eficácia.

São exemplos de controles internos:

- senhas de acesso;
- relatórios indicativos de transações não autorizadas ou acessos não permitidos;
- informações de alterações de arquivos;
- arquivos de informações de controle (AIC);
- *audit trail* (permite a monitoração do processamento de dados);
- rotinas de criptografia de informações sigilosas;
- rotinas operacionais de atualização de cadastros entre outras.

Saiba mais

Stakeholder significa **público estratégico** e descreve uma pessoa ou grupo que tem interesse em uma empresa, negócio ou indústria, podendo ou não ter feito um investimento neles.

Em inglês, *stake* significa "interesse", participação, risco; e *holder,* "aquele que possui". Assim, *stakeholders* também significa **parte interessada** ou **interveniente.** O *stakeholders* é uma pessoa ou um grupo, que legitima as ações de uma organização e que tem um papel direto ou indireto na gestão e resultados dessa mesma organização. Dessa forma, um *stakeholders* pode ser afetado positivamente ou negativamente, dependendo das suas políticas e forma de atuação. Alguns exemplos de *stakeholders* de uma empresa podem ser seus funcionários, gestores, gerentes, proprietários, fornecedores, concorrentes, ONGs, clientes, Estado, credores, sindicatos e diversas outras pessoas ou empresas que estejam relacionadas a uma determinada ação ou projeto.

Fonte: Significados (c2011-2017).

Auditoria e segurança da informação

Quanto melhores forem as formas de controle dos processos internos, maiores serão os resultados operacionais das organizações, portanto, as empresas devem utilizar as auditorias para regularizar rotinas e melhorar seus indicadores de

resultados. Assim, a auditoria da segurança da informação irá proteger os dados, garantir que eles estarão disponíveis quando solicitados e que, sendo corretos, irão gerar o conhecimento empresarial necessário para a tomada de decisão, sem um eventual acesso indevido.

Esse é o mundo ideal, a informação sendo utilizada por quem realmente necessita dela para realizar seus processos.

Eventualmente, ocorrem incidentes nessa segurança, como as tentativas de acesso não autorizado, ataques externos ao processamento de dados, usos não autorizados de estações de trabalho e sistemas operacionais, modificações em sistemas sem autorização ou consentimento do proprietário, enfim ações que causam desrespeito às políticas internas da organização e as políticas do provedor de acesso à rede de computadores.

Esses ataques irão causar danos à empresa, como perdas financeiras e de imagem, transações fraudulentas, acesso a dados confidenciais, furtos e roubos de dados internos e dados de clientes, parada de processamentos e perda da confiança dos fornecedores e clientes aos quais a empresa tem relacionamento.

Para minimizar, isso as políticas de segurança estão seguindo cada vez mais as orientações das auditorias e controlando acessos, tipos de usuários, agindo na melhoria da proteção dos bancos de dados e na navegação na rede de computadores.

A seguir, você verá um passo a passo para a melhoria da segurança da informação:

- **Tipos de usuários:** devem ser definidos em dois tipos, os operacionais ou funcionais, que serão os que irão acessar e utilizar os dados para qualquer tipo de processamento, devendo obedecer a níveis de acesso de acordo com sua atividade dentro da empresa; e os usuários fonte, que são aqueles que originarão os dados que os demais irão utilizar, terão uma maior responsabilidade, pois irão ter a opção de alterarem dados, claro que também com níveis de acesso as informações.
- **Restrições de acesso de dados:** para garantir o processo, é fundamental a empresa ter uma clara política de restrições de acesso, assim melhorando e confiando nos processamentos, essa restrição segue três passos, primeiro identifica o usuário, pela forma de *login* (identificação e senha própria), valida o usuário de acordo com essas informações e concede privilégios de acordo com o nível em que se encontra o usuário.

Assim, o usuário tem acesso individual e acessa o conteúdo ao qual está liberado para acessar, por exemplo, terá conteúdos somente para leitura,

alguns para complementar ou modificar, tudo isso atrelado a sua função dentro da organização. Por exemplo, uma organização do sistema financeiro tem usuários que podem liberar crédito com sua senha e usuários que podem começar o processo de liberação, mas dependem de outro funcionário acessar para completar a liberação, garantindo, com isso, uma melhor performance em segurança do processo. Uma forma atual de controle de acesso é a utilização da biometria, que é uma forma automatizada de verificação e confirmação da identidade de uma pessoa pela análise de uma característica física e única.

A segurança deve ser redobrada nos bancos de dados, pois se ela for quebrada os danos são muito grandes para a empresa. Os bancos de dados devem ter uma parte exclusiva a ser planejada pela alta direção das organizações, sendo que sua segurança deve estar contida na política de segurança da empresa obedecendo a três pontos principais:

- **Segredo:** os usuários não devem ter acesso a informações que não lhes dizem respeito fora de sua atividade, por exemplo, um funcionário da produção ter acesso à formatação do preço de venda de um determinado produto.
- **Integralidade:** um usuário que tem acesso a uma determinada informação para leitura, não pode ter acesso à modificação, por exemplo, um operador de máquina ter acesso à engenharia do produto com condições de alterar algum componente do produto sem a devida análise das consequências desse ato.
- **Disponibilidade:** o sistema tem que ter a robustez necessária para que uma eventual falha não deixe que algum processo não seja realizado, por exemplo, um usuário trava o sistema por uma pesquisa não autorizada e uma nota fiscal deixa de ser emitida ao cliente.

As seguranças nos serviços web são atualmente os mais visados para crimes, portanto devem ter por parte das pessoas e organizações mecanismos de controle e segurança nas diversas camadas, sendo:

- **Segurança na estação:** cuidados em que o usuário realiza a pesquisa dos dados ou alterações em arquivos, utilizando recursos da rede.
- **Segurança no meio de transporte:** a empresa tem que garantir que os dados que circulam dentro de seu domínio estejam protegidos assim como os dados que trafegam para fora da empresa.
- **Segurança nos servidores:** como não é possível ficar off-line as empresas devem investir em proteções aos seus servidores, visto que eles

ficam em contato direto com a rede é salutar que tenham um só ponto de saída e entrada de dados para um melhor monitoramento.

- **Segurança na rede interna:** com objetivo de minimizar os acessos indevidos e a retirada de dados sem autorização.

Uma das mais utilizadas ferramentas para aumentar a segurança da rede no caso de acessos indevidos de fora é a instalação de um Firewall, um sistema utilizado para criação de barreiras seguras entre a web e a rede interna de estações de trabalho.

Complementando assim a política de segurança da informação dentro das empresas, veja na Figura 2 um resumo dessas camadas web e demais.

CAMADA DE ATUAÇÃO	SERVIÇOS	COMPETÊNCIAS
GESTÃO	GESTÃO DA TI, MONITORAMENTO, LICENÇAS DE SOFTWARE, TREINAMENTOS, CONTINUIDADE DO NEGÓCIO, ROI, DESASTRES E RECUPERAÇÃO, TCO	PMP, ITIL, COBIT, GREEN IT, CLOUD
SEGURANÇA	ANTIVÍRUS, BACKUP, CRIPTOGRAFIA, FIREWALL, ETHICAL HACHER, GPO, SEGURANÇA DE DOCUMENTOS, POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	CISSP, SECURITY+
APLICATIVOS	EMAILS, FERRAMENTAS OFFICE, ERPS, SISTEMAS DE BANCOS, SISTEMAS PARA ATENDER GOVERNO.	CERTIFICAÇÃO MICROSOFT OFFICE 365, 2013, SHAREPOINT
SISTEMAS OPERACIONAIS	PROJETO, IMPLANTAÇÃO DE SOLUÇÕES MICROSOFT - PROJETO, IMPLANTAÇÃO DE SOLUÇÕES LINUX	MCITP, MCTS, SERVER+, LINUX+
ATIVOS	ATIVOS DE REDE, DESKTOPS, NOTEBOOKS, IMPRESSORAS, SERVIDORES	A+, CSSA, CCNA, LANCORE, CWNA, BROTHER, PDI+
INFRAESTRUTURA	PROJETO, IMPLANTAÇÃO DE REDES CABEADAS E WIRELESS, RACKS, CABEAMENTO ESTRUTURADO	FURUKAWA, AMP, NETWORK+, AVAYA, MERAKI, BICSI
ENERGIA	ATERRAMENTO, INSTALAÇÃO E MANUTENÇÃO DE NOBREAKS	NHS, PHDONLINE, NBR5410, AUTOCAD, LUMINI

Figura 2. Camadas web.

Fonte: CLS Informática (c2015).

Veja, agora, algumas alternativas para criar camadas de segurança capazes de defender seus ativos contra-ataques (KSECURITY TEAM, 2016).

- **Segurança do e-mail em camadas:** a maioria das violações começam com um e-mail. O e-mail pode conter um link para algum tipo de site de roubo de identidade ou instruções para transferências bancárias. *Phishing*, *ransomware* e *malware* são algumas das ameaças que usam o e-mail como ponto de partida. A saída é apostar em algum *gateway* de e-mail, seja ele um *software* ou uma ferramenta baseada em nuvem. A melhor alternativa é usar **camadas de segurança** para melhorar as artilharias que você já possui.

- **Proteção de DNS:** usar uma ferramenta de proteção de DNS é uma opção contra ataques e exfiltrações de dados que não podem ser ignorados. Todo link que um usuário clica pode atingir um servidor DNS antes de ser aberto efetivamente. É importante ter uma ferramenta que aprenda, a partir desses cliques, produzir um escudo de proteção.
- **Proteção do *endpoint*:** é um importante ponto de defesa contra os ataques. Ferramentas de proteção de *endpoints* variam de ferramentas *antimalware* até VPNs. Você provavelmente precisará de mais de uma, construindo camadas de segurança mais eficientes.
- **Análise do comportamento do usuário:** usar ferramentas que analisam o comportamento do usuário ajuda a acionar o sinal de alerta quando algo de estranho acontece na rede, como um usuário que passa a fazer mais downloads do que o habitual ou acessar pastas em horários que nunca havia acessado. Isso pode indicar que um funcionário esteja praticando ações maliciosas ou tenham tido suas credenciais roubadas.
- **Teste e treinamento contra *phishing*:** o usuário é o elo mais fraco da cadeia de segurança, e precisa ser educado e sensibilizado.

Exercícios

1. Normalmente, os crimes são categorizados como violentos e não violentos. Um exemplo comum de crime não violento é a fraude, pois os fraudadores usam truques e ilusão como "armas". Os crimes são cometidos pelos fraudadores a partir do abuso de poder de sua posição ou do uso indevido da confiança conquistada junto às vítimas.
A fraude ocupacional pode ser entendida como o uso deliberado dos recursos e ativos organizacionais, visando à obtenção de vantagens pessoais. Considerando os diversos tipos de fraude existentes, como o suborno é caracterizado?

a) Quando alguém frauda relatórios ou documentos próprios da empresa por meio da falsificação de assinaturas.
b) Quando alguém não respeita a confidencialidade de um acordo e seus termos.
c) Quando alguém rouba ativos da organização se aproveitando do acesso a sua propriedade.
d) Quando alguém utiliza a posição de poder ou o dinheiro para influenciar outras pessoas.
e) Quando alguém viola os princípios contábeis da organização para gerar benefícios a terceiros.

2. As práticas de gestão de segurança da informação nas organizações visam proteger os dados, as aplicações de *software*, os *hardwares* e as redes. Existem várias estratégias que podem ser utilizadas, mas as empresas necessitam, inicialmente, definir o que precisa ser defendido e fazer uma análise do custo-benefício dessa proteção. Analise as informações a seguir a respeito dos principais objetivos das estratégias de defesa.

I. A detecção de problemas de segurança da informação deve ser realizada com a maior rapidez possível, facilitando o combate ao problema e, até mesmo, reduzindo os danos causados.
II. Um plano de recuperação deve ser montado para reparar os componentes que apresentarem problemas.
III. A correção de problemas deve projetar e configurar corretamente o ambiente tecnológico para se evitar a ocorrência de erros.

Está correto somente o que se afirma em:

a) I.
b) II.
c) III.
d) I, II e III.
e) Nenhuma das afirmações.

3. A proteção do ambiente tecnológico da empresa precisa considerar tanto aspectos da segurança física (acesso e manuseio dos equipamentos) como a segurança lógica (relacionada diretamente ao uso dos softwares, dos dados e das redes). O controle de acesso consiste no gerenciamento das pessoas autorizadas (ou não) a utilizarem equipamentos e *softwares* da empresa. Isso é feito por meio de processos de autorização (possuir o direito de acessar determinado

recurso) e autenticação (comprovar que o usuário realmente é quem ele diz ser). Atualmente, os controles biométricos são bastante utilizados como métodos de autenticação, sendo entendidos como:

a) um método de identificação baseado em algo que apenas o usuário possui, como um cartão inteligente.

b) um método diferenciado para elaboração de diretrizes e monitoramento do seu correto cumprimento.

c) um método manual que envolve a análise individual dos documentos pessoais dos usuários.

d) uma forma automatizada de verificar e confirmar a identidade de uma pessoa por meio da análise de características físicas ou comportamentais.

e) uma forma de descoberta de características pessoais por meio do uso de *logins* e senhas tradicionais no formato textual.

4. O diretor de segurança da informação da Beta S.A., organização atuante no ramo de venda de pacotes turísticos via web, recebeu a informação de que a rede interna sofreu várias ameaças de invasão nos últimos dois dias. Todas essas tentativas de acesso vieram de agentes localizados em redes externas a da organização. Sendo assim, ele solicitou à equipe técnica a instalação de um Firewall para aumentar a segurança da rede e reduzir a probabilidade de acessos externos indevidos na rede interna da empresa. Analise as afirmações a seguir sobre Firewall.

I. A partir do momento em que um Firewall é instalado e devidamente configurado, todo o tráfego da internet que chega à rede interna da empresa passa pela sua verificação.

II. O Firewall é uma ferramenta que se localiza na terceira camada de defesa dos ambientes tecnológicos.

III. O Firewall é um sistema utilizado para criar uma barreira segura entre determinada rede interna (uma intranet, por exemplo) e a internet.

Está correto o que se afirma somente em:

a) I.

b) II.

c) III.

d) I, II e III.

e) Nenhuma das afirmações.

5. A criação de mecanismos de controle é fundamental para que as organizações gerenciem corretamente os acontecimentos em seu ambiente. Nesse sentido, as auditorias exercem papel de grande importância para o sistema de controle da organização, pois atuam como uma camada extra dos outros controles. Na prática, as auditorias ainda podem funcionar como obstáculos a ações criminosas, especialmente aquelas realizadas pelos próprios funcionários da empresa. Analise as afirmações a seguir relacionadas às características básicas da auditoria e identifique a correta.

a) A auditoria auxilia na identificação e preparação de proteções contra todas as ameaças ao ambiente organizacional, estratégia esta que é a mais viável

economicamente.

b) A auditoria interna precisa considerar a estrutura hierárquica da organização, isentando de sua análise os funcionários de alto escalão.

c) O principal objetivo de uma auditoria, seja ela feita por funcionários internos ou por empresas contratadas especificamente para este fim, é encontrar e punir exemplarmente os culpados por ações criminosas na empresa.

d) O uso de funcionários da própria organização como avaliadores em auditorias não é recomendado em qualquer tipo de processo, pois o resultado apresentado sempre será influenciado pelo cargo ocupado pelo auditor.

e) Uma auditoria bem definida e executada é aquela que apresenta isenção e imparcialidade em suas análises e conclusões.

Referências

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil de 1988*. Brasília, DF, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 14 dez. 2016.

BRASIL. *Decreto-lei nº 2.848, de 7 de dezembro de 1940*. Brasília, DF, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 14 ago. 2017.

CLS INFORMÁTICA. *Sobre a empresa*. Vila Velha, c2015. Disponível em: <http://www.clsinfo.com.br/sobre.html>. Acesso em: 14 set. 2017.

LUCHETE, F. *Governo regula uso de algemas e proíbe que mulher fique presa durante parto*. São Paulo: Consultor Jurídico, 2016. Disponível em: <http://www.conjur.com.br/2016-set-27/governo-regula-uso-algemas-proibe-deixar-mulher-presa-parto>. Acesso em: 14 set. 2017.

PORTAL DE AUDITORIA. *A importância da auditoria interna*. Curitiba, 2016. Disponível em: <http://www.portaldeauditoria.com.br/sobreauditoria/A-importanciia-da-auditoria-interna.asp>. Acesso em: 14 set. 2017.

SIGNIFICADOS. *Significado de stakeholder*. Matosinhos: 7Graus, c2011-2017. Disponível em: <https://www.significados.com.br/stakeholder/>. Acesso em: 14 ago. 2017.

TI INSIDE. *Roubo de identidade foi o principal tipo de violação de dados em 2016, afirma relatório*. São Paulo, 2017. Disponível em: <http://convergecom.com.br/tiinside/home/internet/28/03/2017/roubo-de-identidade-foi-o-principal-tipo-de-violacao-de-dados-em-2016-afirma-relatorio>. Acesso em: 14 ago. 2017.

Leituras recomendadas

BEZERRA, F. *Stakeholders*: do significado à classificação. [S.l.]: Portal Administração, 2013-2015. Disponível em: <http://www.portal-administracao.com/2014/07/stakeholders--significado-classificacao.html>. Acesso em: 14 ago. 2017.

CARNEIRO, A. *Auditoria e controle de sistemas de informação*. Rio de Janeiro: FCA, 2009.

LYRA, M. R. *Segurança e auditoria de sistema de informação*. Rio de Janeiro: Ciência Moderna, 2008.

MESQUITA, M. J. S. *Conheça os três tipos de fraude mais comuns no comércio eletrônico*. [S.l.]: Tecmundo, 2014. Disponível em: <https://www.tecmundo.com.br/seguranca/63727-conheca-tres-tipos-fraude-comuns-comercio-eletronico.htm>. Acesso em: 13 ago. 2017.

S2 CONSLTORIA. *Conheça mais 2 tipos de fraude além da corrupção*. São Paulo, c2017. Disponível em: <https://www.s2consultoria.com.br/conheca-mais-2-tipos-de-fraude--alem-da-corrupcao/>. Acesso em: 13 ago. 2017.

SILVEIRA, S. L. A. *Embedded Audit Trail*: aplicador. [S.l.], TOTVS, 2015. Disponível em: <http://tdn.totvs.com/display/public/framework/Embedded+Audit+Trail+--+aplicador>. Acesso em: 14 ago. 2017.

Aplicação de normas, padrões internacionais e certificações

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Compreender o uso das normas e padrões internacionais de segurança da informação.
- Reconhecer as principais normas e padrões internacionais de segurança da informação.
- Identificar as principais certificações para quem trabalha com segurança da informação.

Introdução

A segurança da informação é um assunto que vem se expandindo ao longo dos últimos anos e se tornando uma preocupação constante para organizações de todos os segmentos e portes. Isso se deve, em grande parte, ao aumento do número de incidentes relacionados à segurança, que ocorrem com cada vez mais frequência mundialmente. Os danos trazidos podem ser variados, não somente envolvendo a perda, o roubo, o extravio e as alterações indevidas das informações, mas também atingindo a imagem da empresa perante seus clientes e parceiros.

Em vista disso, muitas são as normas e os padrões internacionais elaborados com o intuito de divulgar boas práticas e diretrizes sobre a segurança da informação, servindo de fundamento para as atividades relacionadas à essa área nas organizações.

Neste capítulo, você vai estudar o uso das principais normas e padrões internacionais de segurança da informação e também as principais certificações para os profissionais da área.

O uso das normas e padrões internacionais de segurança da informação

A área da segurança da informação se relaciona com a proteção de conjuntos de dados ou informações, a fim de preservar o valor que possuem para um indivíduo ou uma organização; ou seja, objetiva preservar informações pessoais ou corporativas. A informação pode estar armazenada para **uso restrito** ou pode ser pública, para que todos a acessem sem restrição.

Fique atento

Os dados não possuem um significado relevante de maneira isolada e representam algo que, a princípio, não possui um sentido, não serve para fundamentar conclusões nem para respaldar decisões. A informação é a ordenação ou a organização de dados de tal forma que eles transmitam um significado e possam ser compreendidos, desde que analisados dentro de um contexto.

A segurança da informação não se restringe somente à informação eletrônica, que tramita em sistemas informatizados com armazenamento eletrônico, e sim a todos os aspectos que envolvem a proteção dos dados e das informações.

Os atributos básicos da segurança da informação dizem respeito à forma como a informação é tratada; são eles: disponibilidade, confidencialidade, autenticidade e integridade. Esse último envolve características dos três anteriores. Esses atributos servem para fundamentar a análise, o planejamento, e a implementação da política de segurança que servirá para um grupo específico de informações a serem protegidas, conforme afirmam Fernandes e Abreu (2014).

Fique atento

Com relação aos atributos da segurança da informação, é importante lembrar que:

- **Disponibilidade** é a característica de um sistema de informação que mantém os seus serviços disponibilizados pelo máximo de tempo possível, sendo resistente a falhas de *hardware*, de *software* e também a falhas de energia.
- **Confidencialidade** é a característica daquela informação que só é divulgada para aqueles indivíduos, processos e máquinas que têm autorização para acessá-la. É a garantia de que a informação trocada entre o emissor e o receptor de uma mensagem vai ter seus dados protegidos durante a transação.
- **Autenticidade** é a característica que diz que, quanto mais próxima da original uma informação que chega ao destinatário for, mais autêntica e confiável ela será. A autenticidade é a garantia de que um indivíduo, um processo ou um computador é quem ele "diz" que é.
- **Integridade** é a característica que envolve o fato de a informação não ter sido alterada de forma não autorizada ou indevida, pois se a informação for alterada por alguém não autorizado, de forma indevida, ela perde a sua credibilidade e o seu valor, tornando duvidosas e imprecisas quaisquer decisões tomadas com base nessa informação e tirando a credibilidade e a confiança em quem a forneceu também. A integridade é a essência da segurança da informação, pois é formada pela disponibilidade, pela confidencialidade e pela autenticidade.

Para definir o nível de segurança da informação, podem ser estabelecidas métricas, que podem utilizar ou não ferramentas e técnicas, mas que servirão para instituir bases para analisar o que precisa ser melhorado com relação à segurança existente.

A segurança de uma informação específica pode ser influenciada por fatores que vão desde o comportamento do usuário que a utiliza até o ambiente ou a infraestrutura onde ela está armazenada, enfrentando ainda indivíduos mal-intencionados que objetivam modificá-la, roubá-la ou, até mesmo, destruí-la.

O nível de segurança necessário pode servir para consolidar uma política de segurança da informação, que poderá ser seguida por uma pessoa ou por toda uma organização, com o objetivo de buscar e manter padrões de segurança ótimos. Para estipular essa política, é preciso levar em conta todos os riscos que estão associados a uma possível falha de segurança, os benefícios trazidos por seguir uma política e também os custos que estão envolvidos na implementação dessa política.

Atualmente, existem muitas ferramentas e sistemas que têm a pretensão de fornecer segurança para informações. Porém, o fato de a organização ou a

pessoa disporem de recursos tecnológicos não é suficiente; é preciso colocar a tecnologia em harmonia com normas, métricas e estratégicas. É por esse motivo que existem referências internacionais e nacionais em gestão da segurança da informação, que oferecem aos profissionais o conhecimento sobre o que existe de mais atualizado na área.

Toda e qualquer informação trabalha com a coleta, o processamento, o armazenamento e a transmissão de informações, por meio da utilização de meios físicos, eletrônicos e, logicamente, por comunicação verbal. Por causa dessa diversidade, muitas são as formas pelas quais as ameaças podem se concretizar, gerando danos e impactos negativos.

Nesse sentido, as práticas de segurança da informação devem ser incluídas o tempo todo na execução das atividades. Quando a segurança da informação é eficaz, ela é capaz de reduzir os riscos e proteger toda a organização das vulnerabilidades e das ameaças.

Segundo Hintzbergen et al. (2018), para que as organizações possam se fundamentar, obtendo diretrizes e princípios que vão guiar suas práticas de segurança da informação, existem diversas normas técnicas, que traduzem padrões internacionais sobre esse assunto.

Foi por causa da preocupação frequente com a garantia da confiabilidade, da autenticidade, da disponibilidade e, principalmente, da integridade das informações, juntamente com o rápido avanço da tecnologia da informação, que foram elaboradas normas, seguindo padrões internacionais, capazes de garantir a segurança da informação em um nível satisfatório, dependendo de cada situação. Essas normas envolvem assuntos como o tratamento das informações, a tecnologia da informação envolvida, a gestão de toda a documentação e, ainda, as técnicas utilizadas para a segurança.

As normas têm o propósito de apresentar as melhores práticas, demonstrar diretrizes, definir princípios, regras e critérios e, principalmente, fornecer critérios para uniformizar os níveis de qualidade de processos, produtos e serviços, na intenção de que sejam eficientes. Em outras palavras, as normas trazem procedimentos e regras a serem seguidos, para assegurar que um processo, um produto ou um serviço seja realizado ou elaborado de forma padronizada e da maneira mais correta possível.

Para que uma organização possa usufruir de tudo o que a segurança da informação oferece, é necessário que os processos, os *hardwares* e os *softwares* envolvidos nos processos supram todas as suas necessidades, levando em consideração os riscos envolvidos nas atividades do negócio. A melhor maneira de assegurar que tudo está sendo feito de forma correta é seguindo

normas estabelecidas para a segurança da informação, pois são específicas para essa área e traçam diretrizes determinadas para as atividades que a envolvem.

As normas técnicas são aprovadas por organismos ou entidades reconhecidas, e as organizações que atenderem aos seus critérios podem, dependendo da norma à qual se vincularam, receber uma certificação de excelência quando forem auditadas.

É cada vez mais frequente o fato de os clientes exigirem, para fechar negócios, que as organizações sejam certificadas ou comprovem que seguem determinadas normas, uma vez que é dessa forma que elas demonstram preocupação com boas práticas internacionais, o que assegura a qualidade de seus produtos e serviços com relação à gestão, à segurança, à inovação e aos processos.

Para que uma organização se torne certificada, ela precisará passar por auditorias realizadas por entidades certificadoras. Estas são responsáveis pela verificação de todos os processos e conformidades, de acordo com determinada norma. O processo de certificação pode variar conforme o tipo de serviço ou produto, ou ainda conforme o porte da organização, mas normalmente ele vai incluir a aplicação das diretrizes da norma, a análise da documentação e a realização de auditorias internas pela organização, para verificar inconsistências e inconformidades e para que possa se adequar.

As principais normas e padrões internacionais de segurança da informação

A BS 7799 é uma norma britânica muito conhecida, que foi desenvolvida por uma instituição inglesa chamada British Standards Institution. Ela foi aprovada pela International Organization for Standardization (ISO) e também pela International Electrotechnical Commission (IEC) para ser utilizada internacionalmente, passando a ser conhecida, no ano 2000, como ISO/IEC 17799, que atualmente traz a padronização para o conceito de segurança da informação.

A norma ISO/IEC 17799 traz um guia de práticas e diretrizes acerca da gestão da segurança da informação, que descreve genericamente quais são as áreas importantes para a implantação e para a manutenção da gestão de segurança da informação em uma organização (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005). A importância dessa norma se deve ao número cada vez mais expressivo de pessoas envolvidas com informações e também aos diversos tipos de ameaças aos quais as informações estão suscetíveis.

Segundo Fernandes e Abreu (2014), os principais objetivos da norma ISO/IEC 17799 são:

- o estabelecimento de um guia de referência para que as organizações possam desenvolver, implementar e avaliar a gestão da tecnologia da informação; e
- a promoção da confiança nas transações comerciais entre organizações.

Para que a gestão dos controles possa ser feita de maneira eficiente, a norma 17799 divide a gestão da segurança da informação em macroáreas, que são: política de segurança, segurança organizacional, classificação e controle dos ativos de informação, segurança de recursos humanos, segurança física e do ambiente, gerenciamento das operações e comunicações, controle de acessos, desenvolvimento e manutenção de sistemas de informação, gestão de continuidade de negócios e conformidade. Dependendo do porte da organização, pode-se perceber que algumas macroáreas não são necessárias, por serem direcionadas a organizações maiores.

Depois disso, a partir de 2005, começaram a ser publicadas as normas da família ISO/IEC 27000, servindo de guia para as melhores práticas de segurança da informação. Elas têm como temas o sistema de gestão de segurança da informação (SGSI), a gestão de riscos, a aplicação de controles, o monitoramento, as revisões, as auditorias, entre outros assuntos. Elas trazem uma forma de fazer a implementação, o monitoramento e o estabelecimento de objetivos.

A certificação e a aplicação das normas da família ISO/IEC 27000 não são obrigatórias, mas a sua utilização traz diretrizes e recomendações para uma gestão eficiente, que vai facilitar a entrega de resultados positivos para a organização.

Dentro da família 27000, a norma 27001 é passível de certificação, e as outras normas servem como fundamento para auxiliar a alcançar resultados positivos, principalmente a norma 27002. As empresas certificadas pela norma ISO 27001 usufruem dos benefícios vindos da sua certificação e podem também passar a exigir que seus fornecedores ou parceiros sejam certificados, como uma garantia de que eles cumpram os princípios fundamentais da segurança da informação, como afirmam Hintzbergen et al. (2018).

A norma ISO/IEC 27001 traz a definição dos requisitos para implementar, operar, monitorar, revisar, manter e melhorar um SGSI. A sua utilização se aplica a qualquer tipo de organização, independentemente do seu setor de atuação ou do seu porte, sendo muito valorizada por aquelas que têm

na segurança das informações um dos fatores cruciais para o sucesso dos seus processos, o que acontece com instituições financeiras e de tecnologia de informação ou instituições públicas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a).

As especificações e a implementação do SGSI de uma organização dependem exclusivamente das suas necessidades, dos seus objetivos, das suas exigências para os níveis de segurança de informação, dos processos executados pelos colaboradores, do seu porte e da sua estrutura. Ou seja, o SGSI deve ser realmente individualizado para cada organização.

Como uma das grandes preocupações das organizações e das suas partes interessadas é o tratamento dado às informações, a implementação da norma ISO 27001 demonstra um compromisso com a segurança da informação, o que representa maior confiabilidade para quem for interagir com a organização certificada. O fato de as organizações certificadas passarem por criteriosos processos de auditoria, feitos por entidades externas credenciadas e idôneas, fará com que os seus parceiros, fornecedores e clientes percebam que, para essas organizações, a integridade das informações é muito importante, e que existe um padrão de exigência elevado para a gestão e a política de segurança da informação na empresa.

Dentre as vantagens que a utilização da norma ISO 27001 pode trazer para uma organização, estão:

- o ganho da confiança das partes interessadas;
- a identificação de oportunidades de melhorias nos processos; e
- a identificação dos riscos, com a definição de controles para administrá-los ou eliminá-los.

Uma outra norma da família ISO 27000 que merece destaque é a norma ISO/IEC 27002, que traz um guia de melhores práticas para a gestão da segurança da informação, assunto fundamental para que a implementação de um SGSI se consolide, garantindo que os processos de segurança se tornem contínuos e estejam alinhados aos objetivos da organização. Ela informa como os controles devem ser definidos e implementados nas organizações, estabelecendo que a sua escolha deve ser baseada na avaliação dos riscos enfrentados pelos ativos mais importantes da organização (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b). Essa norma pode ser aplicada em qualquer tipo de organização, seja ela pública ou privada, independentemente do seu porte, ou se tem ou não fins lucrativos.

Fique atento

A norma ISO/IEC 27002 traz como conceito para a palavra ativo qualquer coisa que tenha importância e valor para a organização e que, por isso, precisa ser protegida de alguma maneira. Os ativos devem ser identificados, avaliados e ter regras para o tipo de uso a que se destinam, para que a organização possa manter um inventário deles.

A norma 27002 tem o objetivo de fornecer diretrizes e princípios para que a organização possa iniciar, implementar, manter e melhorar continuamente a sua gestão de segurança da informação. Conforme Hintzbergen et al. (2018), essas atividades envolvem também a definição, a seleção, a implementação e o gerenciamento de controles, o que vai levar em consideração os riscos enfrentados pela empresa.

Essa norma indica a criação de um documento contendo a política de segurança da informação da empresa, trazendo o conceito de segurança da informação para a organização, seus objetivos e formas de controle. Esse documento ainda deverá informar as responsabilidades de cada um na implementação e na manutenção dessa política. Outro conselho trazido pela norma 27002 é a análise de cada funcionário ou fornecedor contratado, principalmente se o seu trabalho ou atividade envolver algum tipo de informação sigilosa para a empresa. Essa prevenção vai servir para que a organização esteja sempre ciente de suas ameaças com relação à segurança da informação e para que possa diminuir o risco de má utilização, roubo ou fraude nos seus recursos.

Além disso, é importante que as informações sejam mantidas em áreas seguras, com controle de acesso apropriado, o que vai incluir proteções e barreiras físicas e lógicas. O acesso à informação deve ser baseado na importância da informação para o negócio, e a liberação do acesso por perfil e por nível deve ser efetuada conforme a necessidade de cada usuário.

A ISO/IEC 27002 ainda fala sobre a importância de todas as partes interessadas na organização estarem preparadas e informadas acerca dos procedimentos em caso de incidentes de segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b). Para isso, deve ser elaborado um plano de continuidade de negócio, capaz de impedir a interrupção das atividades da empresa e garantir que ela volte à operação normal no menor tempo possível.

Uma organização que faça uso da norma ISO/IEC 27002 poderá ter como benefícios principais:

- a conscientização acerca da segurança da informação para todos os envolvidos com a empresa;
- a identificação e o controle das vulnerabilidades e dos riscos da empresa;
- a oportunidade de ser um diferencial para clientes, parceiros e demais partes interessadas que valorizem uma certificação de padrão internacional;
- a redução de custos originados de incidentes com segurança da informação.

As principais certificações para quem trabalha com segurança da informação

A segurança da informação envolve uma área profissional na qual pode ser comum, apesar de não ser obrigatória, a exigência de uma certificação alinhada ao cargo, à função ou as atividades desempenhadas, ou que se pretende desempenhar. Essas certificações, conforme Fernandes e Abreu (2014), servem para valorizar o currículo dos profissionais que as possuem, representando uma espécie de atestado de que o indivíduo certificado possui grande conhecimento ou experiência nos assuntos relacionados à certificação obtida.

Para auxiliar os profissionais a definir quais as melhores certificações para a sua formação e área de atuação, o Departamento de Segurança da Informação e Comunicações (DSIC), vinculado ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), publicou, em maio de 2013, a norma 17/IN01/DSIC/GSIPR (BRASIL, 2013), sobre a atuação e as adequações para profissionais da área de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal.

Esse documento traz a recomendação de diversas certificações disponíveis para a área da segurança da informação, com a sua classificação baseada no conteúdo de cada uma e na reputação do órgão certificador, servindo de excelente guia para quem já atua ou pretende atuar com segurança da informação profissionalmente e também para empresas e organizações que prestam serviços e consultorias nessa área (SEGINFO, 2018).

Certificação de Auditor Líder ISO 27001

Essa certificação atesta que o profissional é capaz de fazer auditorias em SGSIs e, ainda, coordenar uma equipe inteira de acordo com os preceitos da norma ISO 27001. Sua capacitação para a auditoria vai desde a coleta de informações, passando pelo gerenciamento de riscos e vulnerabilidades, até a elaboração do relatório do que foi auditado.

Essa certificação aborda assuntos como política de segurança, gestão de ativos da organização, gestão de continuidade de negócio, gestão de riscos, segurança física, ambiental e de recursos humanos, entre outros.

Certificação CEH (*Certified Ethical Hacker*)

Uma das principais certificações internacionais, a CEH certifica os profissionais no assunto de *hacking* ético, mas sem enfoque na tecnologia de ataque especificamente, e sim em criptografia, engenharia social, testes de invasão, injeção de código SQL, criação de políticas de segurança, análise e ataque a redes, formas de invasores conseguirem privilégios em redes, entre outros assuntos.

Fique atento

O ***hacker* ético** é um indivíduo que possui habilidades para encontrar vulnerabilidades e pontos fracos em sistemas e utiliza as mesmas técnicas, ferramentas e métodos que um atacante ou indivíduo mal-intencionado utiliza.

Certificação CHFI (*Computer Hacking Forensic Investigator*)

Serve para preparar o profissional para detectar ataques, bem como para extrair as evidências que servirão para comprovar um crime cibernético, de maneira adequada. Serve também para comprovar a capacitação na condução de auditorias, visando a prevenir incidentes de segurança.

Fique atento

A expressão *computer forensic* se refere à aplicação de investigação e técnicas de análise, visando a determinar a evidência legal de uma invasão ou ataque. Essas evidências podem se relacionar com diversos tipos de crimes cibernéticos, como roubo de informações empresariais sigilosas, espionagem corporativa, sabotagem, fraudes e uso indevido de sistemas, programas e demais aplicações.

Certificação CISO (*Chief Information Security Officer*)

Essa certificação tem enfoque na administração da segurança da informação e mostra que o profissional é especialista em gerenciamento de recursos humanos, melhores práticas de segurança, arquitetura para ambientes seguros e avaliação da segurança da informação de qualquer tipo de empresa.

Certificação CISM (*Certified Information Security Manager*)

Essa certificação é própria para quem faz o projeto e gerencia e avalia o programa de segurança da informação das organizações. Ela representa a principal certificação na área de segurança da informação, principalmente porque se destina aos profissionais que já atuam ou pretendem iniciar uma profissão na gestão da segurança da informação.

Para essa certificação, são abordados assuntos como a governança da segurança da informação, a gestão de risco e a conformidade, o programa de gestão e desenvolvimento de segurança da informação e a gestão de incidentes de segurança da informação.

Certificação CISSP (*Certified Information Systems Security Professional*)

Essa é uma das certificações mais desejadas por profissionais da área de segurança da informação, pois atesta que aquele que é certificado tem capacidade de definir a arquitetura, a gestão e os controles que vão assegurar a segurança de ambientes corporativos. A certificação CISSP aborda assuntos como a

computação na nuvem, a segurança móvel, a segurança no desenvolvimento de aplicativos, a gestão de riscos, e muitos outros.

Para que um indivíduo possa obter essa certificação, ele deve ter pelo menos cinco anos de experiência profissional em dois ou mais dos domínios citados como requisitos. Caso o candidato à certificação tenha diploma universitário, a experiência comprovada deve ser de quatro anos.

Os dez domínios requisitados são: controle de acesso, segurança de telecomunicações e redes, governança de segurança da informação, segurança no desenvolvimento de *software*, criptografia, arquitetura e *design* de segurança, segurança de operações, continuidade dos negócios e planejamento para recuperação de desastres, jurídico, regulamentos, investigações e conformidade, e segurança física (ambiental).

Certificação CSA+ (*Cyber Security Analysis*)

Essa é uma certificação internacional que serve para comprovar conhecimentos e habilidades fundamentais necessários para evitar, identificar e combater ameaças à segurança da informação. Ela envolve assuntos como a gestão de ameaças, a gestão de vulnerabilidades e a resposta a incidentes de segurança.

Certificação CSP (*Certified Secure Programmer*)

Essa certificação comprova que o profissional tem a capacidade de desenvolver códigos de programação com alta qualidade, utilizando as melhores práticas de programação existentes, com o intuito de proteger as informações contra vulnerabilidades, uma vez que a maior parte das ameaças aos *softwares* são provenientes de erros de programação e códigos mal escritos.

Certificação ECSA (*EC-Council Security Analyst*)

A certificação CEH é complementada pela ECSA, que tem como fundamento a análise dos dados obtidos durante um teste de invasão. Profissionais como administradores de rede, analistas de segurança da informação, auditores de sistemas e analistas de riscos normalmente encontram muitos benefícios para a carreira obtendo essa certificação. O profissional que obtiver essas duas certificações, CEH e ECSA, vai estar apto a ser um certificado LPT (*Licensed Penetration Tester*).

O assunto dessa certificação são as metodologias, ferramentas e técnicas disponíveis para realizar testes abrangentes de segurança da informação, bem

como o projeto, a proteção e os testes de redes visando a proteger a organização contra ameaças potenciais.

Certificação ISO 27002

Essa certificação serve para quem está começando como profissional da área de segurança da informação. Seu foco está nos conceitos básicos de segurança da informação, auxiliando na compreensão de quais são as informações vulneráveis em uma organização e quais são as medidas mais adequadas para protegê-las. Normalmente essa certificação aborda temas como informação e segurança, ameaças e riscos, abordagem e organização, medidas de segurança, legislação e regulamentação.

Certificação LPT (*Licensed Penetration Tester*)

Serve para atestar que o profissional tem a capacidade de realizar auditorias em segurança de rede e também de realizar testes de invasão, recomendando ações preventivas e corretivas para qualquer vulnerabilidade que for identificada.

Certificação OSCP (*Offensive Security Certified Professional*)

Depois de obter a certificação CEH, o profissional pode desejar ser um certificado OSCP, uma certificação que é conquistada somente por indivíduos que conhecem profundamente o assunto de *hacking*. O profissional que obtém essa certificação comprova ser capaz de compreender um ambiente de segurança desconhecido, elencar objetivos dentro de um escopo definido e ainda documentar resultados em um relatório de nível extremamente profissional.

Certificação *Security+*

Essa é uma certificação internacional que serve para demonstrar competências nas áreas de segurança de redes, conformidade e segurança operacional, ameaças e vulnerabilidades, segurança de aplicações, dados e estações, controle de acesso e identidade, e criptografia.

Ela certifica que o profissional vai estar apto a aplicar os conhecimentos, os conceitos, as ferramentas e os procedimentos de segurança, em caso de incidentes de segurança, e ainda a fazer a antecipação dos riscos de segurança, o que o torna capaz de ser proativo em eventos desse tipo.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 17799*: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002*: tecnologia da informação: técnicas de segurança: código de prática para controles de segurança da informação. Rio de Janeiro, 2013b.

BRASIL. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *17/IN01/DSIC/GSIPR*: atuação e adequações para profissionais da área de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal. 09 abr. 2013. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_17_profissionais_sic.pdf>. Acesso em: 19 jun. 2018.

FERNANDES, A. A.; ABREU, V. F. *Implantando a governança de TI*: da estratégia à gestão de processos e serviços. Rio de Janeiro: Brasport, 2014.

HINTZBERGEN, J. et al. *Fundamentos de segurança da informação*: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

SEGINFO. *Certificações em segurança da informação*. Disponível em: <https://seginfo.com.br/certificacoes-em-seguranca-da-informacao/>. Acesso em: 19 jun. 2018.

Análise de vulnerabilidade em serviços de informação

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Avaliar as vulnerabilidades em serviços de informação.
- Identificar os tipos de vulnerabilidades em serviços de informação.
- Relacionar as diversas ferramentas de análise de vulnerabilidades.

Introdução

A utilização de computadores e da Internet nunca foi tão difundida como na atualidade. As pessoas utilizam a informática para fins de entretenimento, educação, finanças, trabalho, informação, entre outros, e a interrupção de um servidor de Internet ou do acesso a uma rede de computadores pode gerar diversos prejuízos.

Com a popularização dos computadores e a disseminação dos ataques à informação que circula nas redes, a negação de serviços causa grande prejuízo

Neste capítulo, você vai estudar as vulnerabilidades dos serviços de informação e as diversas ferramentas disponíveis para analisá-las.

Vulnerabilidades em serviços de informação

A área da segurança da informação (SI) está envolvida com a proteção de dados e de informações privadas ou públicas, pessoais ou organizacionais, com o objetivo de preservar o valor que possuem para quem é seu titular ou para quem é interessado nelas.

Fique atento

Os principais elementos de que trata a segurança da informação são:

- **Disponibilidade**: é a característica do sistema de informação que mantém os seus serviços disponíveis pelo máximo de tempo possível, resistindo a falhas de *hardware*, de s*oftware* e de energia.
- **Confidencialidade**: trata-se da característica do sistema que garante que a informação será divulgada somente para aqueles indivíduos, processos e máquinas que têm autorização para acessá-la.
- **Autenticidade**: é a garantia de que um indivíduo, processo ou computador é realmente quem ele diz ser.

Além desses atributos essenciais, ainda existe a integridade, que é a base das características da segurança da informação, pois é formada pelas três demais — disponibilidade, confidencialidade e autenticidade.

As atribuições da segurança da informação não se restringem apenas a dados e informações eletrônicas, armazenados em sistemas informatizados, mas dizem respeito também aos sistemas em si e ao ambiente em que estes se encontram. Uma das maiores preocupações da área da segurança da informação são as vulnerabilidades dos sistemas, informatizados ou manuais, e das informações armazenadas por eles.

Fique atento

Os dados não possuem um significado relevante de maneira isolada; eles representam algo que, a princípio, não serve para fundamentar conclusões nem para respaldar decisões. A informação é a ordenação ou a organização de dados de tal forma que eles transmitam um significado e possam ser compreendidos, desde que analisados dentro de um contexto.

Vulnerabilidade é qualquer tipo de fraqueza que reduz a segurança de uma informação, permitindo que uma tentativa de ataque seja bem-sucedida e resultando em uma perda na integridade da informação. Normalmente uma vulnerabilidade envolve uma falha em um sistema, o acesso bem-sucedido de um invasor por meio dessa falha e a capacidade do invasor de explorar a

falha, tendo êxito no seu propósito, seja de roubar, modificar ou excluir as informações.

Algumas das principais ameaças que se apresentam em consequência de vulnerabilidades na segurança da informação são (DANTAS, 2011):

- vírus, cavalos de troia e *worms*;
- *phishing* e *spyware*;
- roubo de informações privadas ou organizacionais;
- prejuízo da performance da rede e dos servidores;
- fraudes financeiras;
- ataques de negação de serviço.

Uma das principais ameaças à segurança da informação é chamada de negação de serviço. Esse é um tipo de ataque que consiste na interrupção e no estrago de um serviço de dados ou de acesso à informação. Todo e qualquer ataque que faça um computador ou um sistema ficar indisponível ou impossibilitado de executar suas funcionalidades básicas consiste em um ataque de negação de serviço, conforme explicam Goodrich e Tamassia (2013).

Em outras palavras, toda situação ou evento que impedir uma máquina ou um sistema de funcionar de maneira adequada, na sua plenitude de potencialidades, estará configurando um ataque de negação de serviço. Um bom exemplo desse tipo de ataque é um *spam* de envio de *e-mails*, com quantidade de envios suficiente para lotar a caixa de entrada e tornar lento ou indisponível o servidor de correio eletrônico. Outro exemplo de ataque por negação de serviço atinge o comércio eletrônico. Tipicamente, ele envolve o fato de a largura de banda das redes ser finita, ou seja, de o número de conexões de clientes a um servidor *web* ser limitado. Cada conexão de um cliente com um servidor precisa de uma determinada capacidade de rede para funcionar; quando um servidor já utilizou toda a sua capacidade, ele não responderá a novas requisições, que serão descartadas e impedirão que clientes acessem os recursos desse servidor. Durante um ataque de negação de serviços, uma grande quantidade de máquinas ligadas à Internet supera a capacidade de requisições dos provedores de serviços *on-line*. Existem muitas ferramentas utilizadas pelos atacantes para fazerem pedidos contínuos de pacotes para os servidores, ou ainda para fazerem o envio contínuo de *spam*. Entre essas ferramentas, está a T50 Sukhoi PAK FA Mixed Packet Injector, criada por um brasileiro e com único propósito fazer com que um servidor seja paralisado ou fique totalmente desestabilizado por requisições contínuas.

As ferramentas utilizadas para os ataques de negação de serviço, além de serem múltiplas, são de difícil detecção. Apesar disso, é possível que o usuário preste atenção ao tráfego da rede na qual sua máquina ou servidor está se conectando no momento, pois, se o computador estiver enviando pacotes continuamente, sem que o usuário esteja acessando qualquer serviço, pode ser um indício de que sua máquina é um "zumbi". Além disso, a conexão com a Internet pode apresentar lentidão fora do comum, sem que se esteja realizando qualquer tarefa simultânea.

Fique atento

Uma máquina zumbi é uma máquina escravizada, que está sendo utilizada por um atacante em um ataque de negação de serviço do tipo distribuído.

Normalmente, um ataque de negação de serviço não pode ser evitado com 100% de certeza de que não vai se consolidar. Algumas medidas podem ser utilizadas em conjunto, para que se possa diminuir o risco de acontecer o ataque, segundo McClure, Scambray e Kurtz (2014):

- Implementação de filtragem de entrada: consiste em bloquear o tráfego de entrada proveniente de intervalos de endereço privados e reservados, que geralmente são considerados inválidos e, por isso, não devem ser utilizados como endereço de origem válido.
- Implementação de filtragem de saída**:** consiste em impedir que pacotes IP falsificados saiam da rede, permitindo que apenas os endereços de origem válidos dos sites na Internet consigam entrar e bloqueando todos os demais endereços de origem considerados inválidos.
- Autenticação de atualizações de roteamento: significa que não deve ser permitido acesso não identificado na infraestrutura de roteamento. A maioria dos protocolos de roteamento não possui mecanismo de autenticação e, se possui, é muito insuficiente, o que se torna uma situação excelente para que invasores falsifiquem os endereços IP de origem e criem condições para ataques de negação de serviço. Quem se torna vítima de um ataque desse tipo tem o seu tráfego roteado pela rede dos invasores ou para uma rede que não existe.

- Implementação de redes de escoamento: consiste na filtragem de endereços inválidos, enquanto se pode monitorar de onde se originam. Com a configuração de um roteador que serve somente para identificar endereços de destino falsos, pode-se conseguir bloquear a sua autenticação na rede.

O ataque de negação de serviços faz com que os recursos da rede sejam utilizados ostensivamente, fazendo com que usuários verdadeiros fiquem impossibilitados de utilizá-los. Não é uma invasão a um sistema, mas sim uma impossibilidade de utilização, por sobrecarga.

Tipos de vulnerabilidades

Como vimos, as vulnerabilidades em serviços podem causar ataques de indisponibilidade chamados de negação de serviço, que têm como propósito interromper ou atrapalhar a realização de atividades oriundas de usuários legítimos em máquinas ou servidores para os quais seu acesso é permitido. A negação de serviço é gerada pela criação artificial de inúmeras solicitações falsas às máquinas ou servidores. Funciona como se milhares de pessoas chegassem em um restaurante ao mesmo tempo e chamassem os atendentes disponíveis sem a intenção de realmente fazerem um pedido, apenas para impedirem que clientes verdadeiros pudessem pedir suas refeições.

O ataque de negação de serviço pode ser dividido em dois grandes grupos, asseguram Nakamura e Geus (2007):

- **Negação de serviço** (DoS, do inglês *Denial of Service*): é o ataque mais comum, que envolve a tentativa de gerar sobrecarga em servidores de rede ou computadores comuns para que os serviços, ou recursos do sistema, fiquem indisponíveis para aqueles usuários que deveriam ter a possibilidade de utilizá-los normalmente. Via de regra, o atacante utiliza técnicas e ferramentas em uma máquina poderosa, com boa configuração e boa capacidade de processamento, que seja capaz de enviar múltiplas solicitações e pedidos de pacotes para a sua máquina-alvo, com a ideia de sobrecarregá-la e impedir seu perfeito funcionamento (Figura 1). Dessa forma, os seus usuários não vão mais conseguir acessar informações, e terão negados os seus serviços. No ataque DoS, são atingidos computadores com pouca banda e especificações técnicas mais simples.

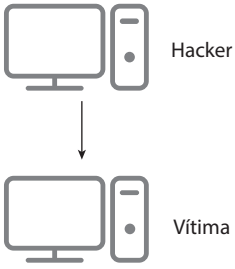

Figura 1. Funcionamento de um ataque de negação do tipo DoS.
Fonte: Adaptado de Canaltech (c2018, documento online).

- **Negação de serviço distribuída** (DDoS, do inglês *Distributed Denial of Service*): nesse tipo de ataque, um computador, conhecido como máster, pode controlar milhões de outros computadores, chamados de zumbis. O computador máster faz com que os computadores zumbis ataquem, todos ao mesmo tempo, uma máquina-alvo, fazendo com que a sobrecarga seja muito mais rápida e violenta (Figura 2). Essa sobrecarga faz com que o servidor paralise e não consiga atender a mais nenhum outro pedido, ou até mesmo que ele seja reinicializado. A negação de serviço distribuída tem esse nome, então, pelo fato de distribuir o ataque em diversas máquinas auxiliares.

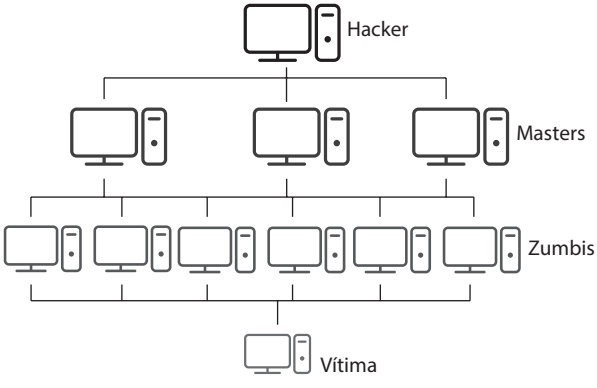

Figura 2. Funcionamento de um ataque de negação do tipo DDoS.
Fonte: Adaptado de Canaltech (c2018, documento online).

Um ataque de negação de serviço, por si só, é perigoso e prejudicial aos usuários e aos computadores ligados à rede. No entanto, a forma distribuída se apresenta como ainda mais prejudicial, pois as máquinas zumbis podem estar espalhadas e nem mesmo ter relação entre si, ou seja, podem estar localizadas em cidades e redes diferentes, bastando apenas que estejam conectadas ao computador master, controlado pelo atacante.

Além dessa classificação, os ataques de negação de serviço ainda podem ser divididos, conforme Dantas (2011), em:

- **Ataque por inundação**: é o tipo mais comum de ataque de negação de serviço, que acontece pela inundação do tráfego TCP SYN. Esse tráfego explora a abertura de conexões do protocolo TCP, que é utilizado em serviços que precisam de entrega de dados precisa e confiável e é iniciado pela troca de parâmetros entre o cliente e o servidor. Nesse tipo de ataque, um cliente solicita uma abertura de conexão, e o servidor processa esse pedido e faz a alocação de memória para armazenar as informações do cliente. Depois disso, um pacote TCP SYN é enviado em resposta ao cliente, levando a notificação para ele de que seu pedido de conexão foi aceito; o cliente, então, devolve um pacote ACK, que vai servir para completar a abertura da conexão. É a partir daí que os recursos da máquina da vítima vão poder ser explorados da forma que o atacante quiser.
- **Ataque reflexivo ou por amplificação**: é semelhante ao ataque por inundação, mas conta com um elemento que faz um intermédio entre o atacante e a vítima. Esse elemento intermediário vai servir para duplicar o tráfego de ataque entre o atacante e a vítima, o que dificulta muito a identificação dos atacantes, uma vez que o tráfego que chega na máquina vítima tem sua origem no intermediário, e não no atacante real. Nesse ataque, o atacante envia uma requisição ao elemento intermediário usando o endereço da vítima, em vez do seu próprio. O intermediário, então, não consegue autenticar a origem da requisição e envia uma resposta direta para a vítima, e não para o atacante.
- **Ataque na infraestrutura da rede**: é o tipo de ataque que não atinge a vítima de forma direta, mas sim os servidores que traduzem os nomes dos sites utilizados pelos usuários para concluir seu acesso. Um ataque de serviço na resolução dos nomes vai gerar a negação do serviço. Esse ataque é comum de ser realizado contra grandes sites da Internet, como Yahoo, Microsoft, Terra, Amazon, entre tantos outros.

- **Ataque de vulnerabilidade**: esse tipo de ataque pretende unicamente deixar a vítima impossibilitada de realizar qualquer atividade; uma das principais maneiras de o atacante conseguir isso é explorando alguma vulnerabilidade na máquina, nos recursos e nos serviços da vítima.
- **Ataque de protocolo**: esse tipo de ataque é caracterizado pelo consumo excessivo dos recursos da vítima, por meio da exploração de alguma característica específica, ou de alguma vulnerabilidade na implementação de um protocolo instalado na máquina da vítima.

Ferramentas de análise de vulnerabilidades

Um ataque de negação de serviço, principalmente do tipo distribuído, é um ataque de disponibilidade muito difícil de combater. Normalmente, as requisições de serviço e as tentativas de conexão falsas se misturam com as verdadeiras ou legítimas, fazendo com que estas tenham uma chance muito pequena de conseguir uma resposta do servidor, como explicam McClure, Scambray e Kurtz (2014).

Existem inúmeras ferramentas que auxiliam os atacantes a realizarem ataques de negação de serviço, e muitas delas são obtidas facilmente pela Internet. Por meio dessas ferramentas de ataque, é muito fácil fazer com que as tentativas de conexão e as requisições se passem por tráfego legítimo, o que dificulta a análise por parte da vítima, que não consegue diferenciar as requisições falsas das verdadeiras. Mesmo se a tarefa de diferenciar requisições fosse algo fácil, ainda assim seria complicada nesse caso, em razão da quantidade de requisições, pois são inúmeras e provenientes de inúmeros lugares, espalhados geograficamente por meio de máquinas conectadas à Internet.

Apesar de existirem ferramentas para analisar a vulnerabilidade a ataques contra serviços por meio da rede, esses ataques não deixam de ser um grande problema. Para as empresas, eles não só impedem o simples acesso de clientes aos sites, como também a possibilidade de fechar negócios. Para pessoas físicas, eles impedem a realização de tarefas simples e também a possibilidade de trabalhar de casa.

A intenção dos profissionais da área de segurança da informação, quando precisam prevenir e enfrentar ataques de disponibilidade do tipo negação de serviços, é simplesmente fazer com que seus servidores e computadores continuem atendendo a requisições de serviços daqueles usuários que forem legitimados a utilizá-los. Nesse sentido, ser preventivo é muito melhor do que ser corretivo; ou seja, se for possível, prevenir um ataque será melhor do que

remediar seus efeitos. Dessa forma, existem basicamente duas formas para prevenir ataques de negação de serviço, que são: evitar que eles aconteçam ou aumentar a capacidade do sistema como um todo, visando a resistir ao ataque e à sobrecarga de tráfego.

Para prevenir um ataque de negação de serviços, pode-se analisar os sistemas, tanto quanto for possível, tomando uma das seguintes medidas, conforme explicam Nakamura e Geus (2007):

- Melhorar a programação e a codificação dos sistemas informatizados, o que vai aumentar o nível de segurança das aplicações. Quanto mais o desenvolvedor for treinado para evitar esse tipo de ataque, mais ele vai codificar seus programas de maneira clara e segura, evitando a incidência de ataques.
- Exigir mais da etapa posterior ao desenvolvimento do *software,* o que envolve a atividade de teste dos programas, o que vai auxiliar os programadores, por meio de seus erros, a escreverem códigos sem vulnerabilidades específicas de segurança.
- Utilizar ferramentas automatizadas para varredura e verificação dos programas e serviços, o que vai servir para aumentar a capacidade de encontrar erros, falhas e vulnerabilidades.
- Utilizar servidores *proxy*, o que consiste em uma das maneiras mais comuns de prevenção contra esse tipo de ataque. Os servidores *proxy* são responsáveis por analisar as requisições às máquinas da rede. Nesse caso, existe uma ponte entre a Internet e o computador vítima, sendo que o *proxy* filtra o tráfego indesejado, permitindo que tudo aquilo que for tráfego verdadeiro, possa passar.

Independentemente de ser a vítima final de um ataque de negação ou de ser uma vítima que trabalha como um zumbi do master, a serviço do atacante, a defesa é bem semelhante. É importante ter disponíveis ferramentas ou técnicas que permitam analisar a rede e os dados que trafegam, de um jeito que torne possível detectar possíveis anormalidades.

A detecção de um ataque pode ser uma atividade bem complicada de executar, principalmente porque ele pode ser imperceptível, principalmente no início, enquanto ainda não conseguiu parar totalmente o servidor, cessando seu funcionamento e impedindo novas respostas às requisições. A lentidão na conexão e na resposta dos serviços, características da ocorrência de um ataque de negação de serviços, pode ser confundida com problemas no provedor do serviço de Internet, ou mesmo com dificuldades de processamento

do computador. Dificilmente o usuário vai se dar conta imediatamente de que pode se tratar de um ataque DoS ou DDoS.

Por isso, é preciso implementar medidas que façam a análise e a identificação de atividades maliciosas na rede, possibilitando o diagnóstico e a caracterização de um ataque assim que uma anormalidade seja detectada, partindo de um cenário típico do tráfego daquela rede específica. Dessa maneira, pode ser possível, também, investigar de onde o ataque é proveniente, mesmo que não seja possível chegar ao atacante original, mas identificando os zumbis e os elementos intermediários.

Os ataques de negação de serviço são bastante comuns, mas normalmente têm alvos bem definidos para os atacantes, o que significa que nem todos os usuários que navegam pela rede serão necessariamente vítimas. Por isso, pode ser mais fácil reagir contra um possível ataque do que preveni-lo. As vítimas não são necessariamente as finais, mas podem ser também aquelas que servem como zumbis dos atacantes originais. Geralmente, as vítimas finais de um ataque de negação de serviço são:

- *sites* e servidores de agências de inteligência e de segurança, como o FBI e a NASA;
- *sites* ligados ao terrorismo;
- *sites* ligados a partidos políticos;
- *sites* e servidores de governos de países;
- *sites* ligados à pornografia;
- servidores de *sites* para Internet;
- *sites* de comércio eletrônico maiores e mais famosos;
- *sites* ligados a jogos de azar;
- servidores ou portais de Internet.

Independentemente da escolha entre prevenir ou reagir contra um ataque, o que importa mesmo é que a medida tomada seja efetiva e funcione, evitando prejuízos. É importante ter em mente que a medida adotada deve ser capaz de enfrentar qualquer tipo de ataque de negação que se apresente. Isso porque novas formas de ataque surgem todos os dias, muito por causa da criatividade dos indivíduos maliciosos e pela motivação que eles possuem em destruir as formas de defesa existentes. Além disso, a medida tomada deve ser responsável por manter o acesso de usuários legítimos a serviços e recursos da rede e dos servidores, como defendem Laufer et al. (2005).

Se a escolha for reagir contra um ataque, isso não quer dizer que não se deve estar preparado para agir, mas sim que a análise do cenário deve

ser criteriosa. Deve haver diagnóstico e identificação do ataque, bem como planejamento do que deve ser feito em caso de um ataque ser bem-sucedido. Para controlar e estar preparado em casos de ataques de negação de serviços, pode-se utilizar o seguinte guia, produzido pelo CERT ([2018]), que envolve os seguintes passos:

- Preparação: envolve o fato de que, para que seja possível fazer a gestão da segurança da informação, é preciso estar preparado para isso. Essa etapa envolve obter um mapa atualizado da rede, conhecer a sua infraestrutura, conhecer a sua rotina de tráfego, criar procedimentos adequados e identificar pessoas que podem ser contatadas em caso de ataque.
- Identificação: envolve a detecção do ataque e a determinação do seu alcance e das partes envolvidas.
- Contenção: consiste em executar medidas, nos dispositivos da rede, para evitar que o tráfego malicioso afete o funcionamento dos serviços, por meio do bloqueio ou do redirecionamento das requisições falsas, ou ainda buscando novos canais de conexão entre os usuários legítimos e os servidores.
- Remediação: consiste em deter o ataque; quanto mais rápido isso acontecer, menor será o impacto e menores serão os prejuízos trazidos. Para isso, é preciso conhecimento dos procedimentos corretos a serem adotados, e rapidez e agilidade para realizá-los.
- Recuperação: envolve a volta dos serviços ao seu estado original de funcionamento, o que implica em ter realizado as fases anteriores de maneira satisfatória, para que não aconteçam problemas no retorno ao funcionamento normal.
- Pós-ataque: envolve a análise do que aconteceu, por meio da documentação de todos os detalhes do ataque, da discussão das lições aprendidas e da verificação do que poderia ser evitado, e, ainda, o retorno à primeira etapa, a da preparação, para estar melhor preparado para uma nova ocorrência de ataque.

Referências

CANALTECH. *Ataque de Negação de Serviço.* c2018. Disponível em: < https://imagens.canaltech.com.br/70031.104739-Ataques-DDoS.jpg>. Acesso em: 23 jul. 2018

CERT. *DDoS incident response*. [2018]. Disponível em: <https://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf>. Acesso em: 22 jul. 2018.

DANTAS, M. L. *Segurança da informação*: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

GOODRICH, M. T.; TAMASSIA, R. *Introdução à segurança de computadores*. Porto Alegre: Bookman, 2013.

LAUFER, R. P. et al. Negação de serviço: ataques e contramedidas. In: *Livro-Texto dos Minicursos do V Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. Florianópolis, Brasil: SBSeg'2005, 2005. p. 1-63.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. *Hackers expostos:* segredos e soluções para a segurança de redes. Porto Alegre: Bookman, 2014.

NAKAMURA, E. T.; GEUS, P. L. *Segurança de redes em ambientes cooperativos*. São Paulo: Novatec, 2007.

Planejamento e anatomia de ataques

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Conceituar tipos de ataques.
- Identificar os tipos de ataques.
- Planejar a anatomia de ataques.

Introdução

É provável que você já tenha passado pela seguinte situação: ao acessar o seu correio eletrônico, deparou-se com inúmeros e-mails indesejados, ou mesmo com mensagens aparentemente verídicas, que apontam para um *link* que fará um *download* indesejado. Estes são apenas alguns exemplos de ataques maliciosos, antes reservados aos ambientes corporativos, mas que atualmente se tornaram corriqueiros no cotidiano do usuário comum.

Neste capítulo, você vai estudar os principais tipos de ataques que ocorrem na rede, as etapas de seu planejamento e os programas a eles relacionados. Você vai verificar também os conceitos mais relevantes que norteiam o assunto e, por fim, vai identificar a anatomia dos ataques considerados ativos e passivos.

Tipos de ataques: conceitos

Ao ouvirmos ou lermos o termo "ataque", sabemos imediatamente que algo, independentemente do que seja, provocará alguma ameaça a algo ou alguém; sempre haverá pelo menos um prejudicado na história. Com o passar dos anos, no contexto computacional e tecnológico, esse tipo de situação tem se tornado habitual. Até recentemente, esses ataques eram mais comuns em ambientes corporativos, devido às informações desses locais serem mais relevantes e

atreladas a valores financeiros. Hoje, no entanto, podemos verificar diversos casos também no cotidiano das pessoas.

Se engana quem pensa que os dados presentes em seu computador ou em seu *smartphone* não são de interesse de terceiros. Hoje, o que temos de mais valioso são nossas informações. Dessa forma, entre esses terceiros interessados, enquadram-se empresas em busca de colher a maior quantidade possível de informações de seus clientes e possíveis clientes. Trata-se de informações sobre como você se comporta, o que você pesquisa, o que você come, quais marcas você veste, quais suas preferências pessoais, entre outras.

Saiba mais

Segundo Stallings (2008), uma ameaça pode ser definida como potencial para violação da segurança quando há circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Um ataque à segurança do sistema é derivado de uma ameaça inteligente, ou seja, um ato inteligente, que é uma tentativa deliberada de burlar os serviços de segurança.

Em 2018, diversos dados pessoais de usuários de uma renomada rede social foram acessados de forma indevida. Nos dois anos anteriores também houveram ataques a redes nacionais, afetando o funcionamento de bancos, universidades e, até mesmo, de alas hospitalares. Se você pesquisar quantos ataques aconteceram nos últimos anos, perceberá que estamos suscetíveis a esse tipo de acontecimento a qualquer momento. Por esse motivo, é importante que saibamos nos precaver o máximo possível, para não nos tornarmos alvos fáceis.

Pode-se afirmar que existem ataques ativos e passivos. Um ataque passivo fará a descoberta e o consequente uso de informações, porém sem a intenção de afetar os recursos que estão sendo utilizados. Por outro lado, o ataque ativo, além de fazer descobertas sobre os recursos da máquina, acabará afetando também o seu funcionamento, na maioria das vezes de forma maliciosa.

Com a diversidade de dispositivos e, consequentemente, de tecnologias disponíveis, os ataques podem se dar de diferentes formas, seja por meio de um simples e-mail, seja pela invasão da rede. Algumas etapas desses ataques são a análise do perfil do alvo, a varredura e a enumeração, não se limitando apenas a estas, pois, como foi comentado, existe uma grande variedade de ataques cibernéticos.

De acordo com McClure, Scambray e Kurtz (2014), a análise do perfil sistemático e metódico de uma organização permite aos invasores criarem um quadro quase completo de seu sistema de segurança da informação. Usando uma combinação de ferramentas e técnicas, acompanhada de uma boa dose de paciência e ordenação mental, os invasores podem tomar uma empresa até então por eles desconhecida e reduzi-la a uma gama específica de nomes de domínio, blocos de rede, sub-redes, roteadores e endereços IP individuais de sistemas diretamente conectados à Internet, além de muitos outros detalhes pertinentes à postura de segurança da companhia. Embora existam muitos tipos de técnicas de identificação de perfil, elas se destinam principalmente à descoberta de informações relacionadas aos seguintes ambientes: Internet, intranet, acesso remoto e extranet. A seguir, no Quadro l, são listadas algumas das informações que os invasores são capazes de identificar durante a análise do perfil de uma empresa, para o planejamento de um ataque.

Quadro 1. Informações interessantes de perfil que os invasores podem identificar

Tecnologia	Informações identificadas
Internet	Nomes de domínio
	Blocos de rede e sub-redes
	Endereços IP específicos de sistemas que podem ser acessados pela Internet
	Serviços TCP e UDP em execução em cada sistema identificado
	Arquitetura de sistema (por exemplo, Sparc *vs.* x86)
	Mecanismos de controle de acesso e listas de controle de acesso (*access control lists — ACLs*) relacionadas
	Sistemas de detecção de intrusão (*intrusion detection systems — IDSs*)
	Enumeração de sistemas (nomes de usuário e grupo, *banners* de sistema, tabelas de roteamento e informações de *simple network management protocol* — SNMP —, em português, protocolo simples de gerência de rede)
	Nomes DNS dos equipamentos

(*Continua*)

(*Continuação*)

Quadro 1. Informações interessantes de perfil que os invasores podem identificar

Tecnologia	Informações identificadas
Intranet	Protocolos de redes em uso (por exemplo, IP, IPX, DecNET, etc.)
	Nomes de domínio internos
	Blocos de rede
	Endereços IP específicos de sistemas que podem ser acessados pela Internet
	Serviços TCP e UDP em execução em cada sistema identificado
	Arquitetura de sistema (por exemplo, SPARC *vs.* x86)
	Mecanismos de controle de acesso e ACLs relacionadas
	Sistemas de detecção de intrusão
	Enumeração de sistemas (nomes de usuários e grupos, *banners* de sistema, tabelas de roteamento e informações SNMP)
Acesso remoto	Números de telefone analógicos/digitais
	Tipo de sistema remoto
	Mecanismos de autenticação
	VPNs e protocolos relacionados (IPSec e PPTP)
Extranet	Nomes de domínio
	Origem e destino de conexões
	Tipo de conexão
	Mecanismos de controle de acesso

Fonte: Adaptado de McClure, Scambray e Kurtz (2014, p. 9).

Ou seja, a análise do perfil permite que as informações mais relevantes para o ataque sejam selecionadas. Já a varredura, que seria a próxima etapa, é responsável pela análise de pontos em que o ataque pode ser realizado e como ele pode ocorrer. Ainda sob o ponto de vista de McClure, Scambray e Kurtz (2014), a principal diferença entre as técnicas de análise do perfil e de varredura e a enumeração é o nível de intrusão. A enumeração envolve conexões ativas com sistemas e consultas direcionadas.

Grande parte das informações obtidas por meio da enumeração pode parecer inofensiva à primeira vista. Contudo, as informações vazadas das brechas apontadas a seguir podem ser sua ruína, conforme ilustraremos ao longo deste capítulo. Em geral, as informações obtidas por meio da enumeração incluem:

- nomes de conta de usuário (para formular ataques subsequentes de adivinhação de senha);
- recursos compartilhados, muitas vezes mal configurados (por exemplo, compartilhamento de arquivos não protegidos); e
- versões de *software* antigas, com conhecidas vulnerabilidades na segurança (como servidores web com estouros de *buffer* remotos).

Uma vez enumerado um serviço, normalmente é questão de tempo até que o invasor comprometa o sistema, parcial ou totalmente. Fechando essas brechas, que são facilmente corrigidas, você elimina o primeiro ponto de apoio do atacante, conforme explicam McClure, Scambray e Kurtz (2014).

As três etapas do planejamento do ataque aqui mencionadas podem ser colocadas em prática de diversas maneiras. Cada uma traz consigo complexidades relacionadas ao modo como serão executadas, ou seja, como serão utilizadas para a aplicação de algum tipo de ataque. No próximo tópico falaremos sobre a identificação de alguns dos principais tipos de ataques e suas particularidades.

Fique atento

Conforme McClure, Scambray e Kurtz (2014), normalmente os *scanners* de vulnerabilidade automatizados contêm, e atualizam regularmente, enormes bancos de dados de assinaturas de vulnerabilidade conhecidas para basicamente todas as informações que estão sendo recebidas em uma porta de rede, inclusive sistemas operacionais, serviços e aplicativos web. Eles podem detectar vulnerabilidades no *software* do lado do cliente, mediante credenciais suficientes, uma estratégia que pode ser útil em estágios posteriores do ataque, quando o invasor pode estar interessado em expandir ainda mais sua base de operações, comprometendo contas adicionais de usuário privilegiado.

Identificação dos tipos de ataques

Podemos notar que o debate sobre os tipos de ataques pode ser algo bastante extenso, pois, como comentamos, a diversidade se faz presente tanto nos tipos quanto nos contextos onde eles podem estar inseridos. Segundo Stallings (2008), podemos destacar alguns dos principais programas maliciosos existentes, os quais estão expostos no Quadro 2 a seguir.

Quadro 2. Terminologia dos programas maliciosos

Nome	Descrição
Vírus	Anexa-se a um programa e propaga cópias de si mesmo a outros programas
Verme (*worm*)	Programa que propaga cópias de si mesmo a outros computadores
Bomba lógica	Dispara uma ação quando ocorre uma determinada condição
Cavalo de Troia	Programa que contém uma funcionalidade adicional inesperada
Backdoor (*trapdoor*)	Modificação de programa que permite o acesso não autorizado à funcionalidade
Exploit	Código específico para uma única vulnerabilidade ou um conjunto de vulnerabilidades
Downloader	Programa que instala outros itens em uma máquina sob ataque; normalmente, é enviado em um e-mail
Auto-rooters	Ferramentas maliciosas de *hacker* usadas para invasão de novas máquinas remotamente
Kit (geradores de vírus)	Conjunto de ferramentas para gerar novos vírus automaticamente
Programas de *spam*	Usados para enviar grandes volumes de e-mails indesejados

(*Continua*)

(*Continuação*)

Quadro 2. Terminologia dos programas maliciosos

Nome	Descrição
Flooders	Usados para atacar sistemas de computador em rede com um grande volume de tráfego, visando a executar um ataque de negação de serviço (DoS)
Keyloggers	Capta teclas digitadas em um sistema comprometido
Rootkit	Conjunto de ferramentas de *hacker* usadas após o atacante ter invadido um sistema de computador e obtido acesso em nível de *root*
Zumbi	Programa ativado em uma máquina infectada que é preparado para desferir ataques a outras máquinas

Fonte: Adaptado de Stallings (2008, p. 428).

Stallings (2008) conceitua *software* malicioso como aquele intencionalmente incluído ou inserido em um sistema com um propósito prejudicial. Segundo o autor, esse tipo de *software* pode ser identificado e classificado por meio de algumas características, dentre elas a necessidade de o programa necessitar ou não de um hospedeiro. O *software* que não tem essa necessidade é considerado independente. Ainda conforme Stallings (2008), *software* que necessita de um hospedeiro é um fragmento de programa que não podem existir independentemente de um programa de aplicação, de um utilitário ou de um programa do sistema, por exemplo: os vírus, as bombas lógicas e os *backdoors*. Ainda conforme o autor, outro tipo de *software* consiste em um fragmento de programa que pode ser considerado independente ou não, e que, quando executado, pode produzir uma ou mais cópias de si mesmo para serem ativadas mais tarde, no mesmo sistema ou em algum outro sistema; como exemplos, podemos citar os vírus e os vermes (*worms*).

A persistência nas tentativas de acesso a informações é tão presente que existe até um termo utilizado para essas tentativas aplicadas às redes corporativas: ameaças persistentes avançadas (APTs, do inglês *advanced persistent threats*). Para McClure, Scambray e Kurtz (2014, p. 318):

> [...] uma APT é, basicamente, outro termo para descrever um *hacker* que está utilizando ferramentas avançadas para comprometer um sistema — mas com uma característica adicional: maior determinação. O objetivo da maioria dos *hackers* é obter acesso, fazer suas atividades e subtrair as informações que

> servem aos seus propósitos. O objetivo de uma APT é lucrar em cima de alguém em longo prazo, mas ela não precisa ser "avançada" ou "persistente" para satisfazer seus objetivos [...] As APTs podem ter como alvo organizações sociais, políticas, governamentais ou industriais — e frequentemente têm. Informação é poder e o acesso a (ou o controle de) informações competitivas é poderoso (grifo nosso).

De maneira genérica, as APTs podem ser classificadas em dois grupos, de acordo com os objetivos dos invasores. O primeiro grupo consiste em atividades criminais que visam a obter informações de identidade pessoal e/ou financeiras e, oportunamente, informações corporativas, que podem ser utilizadas para cometer fraude financeira ou roubo de identidade. O segundo grupo está a serviço de interesses competitivos da indústria ou serviços de inteligência patrocinados pelo Estado (às vezes, os dois não estão dissociados). Essas atividades visam a obter informações patenteadas e, normalmente, privadas, incluindo propriedade intelectual e segredos comerciais, para apresentar produtos e serviços competitivos no mercado ou planejar estratégias para concorrer ou responder à capacidade das organizações das quais roubam informações, conforme explicam McClure, Scambray e Kurtz (2014).

Saiba mais

Sobre o grupo de *hackers* denominado Anonymous, McClure, Scambray e Kurtz (2014, p. 325) dizem que:

> O Anonymous surgiu em 2011 como um grupo de *hackers* muito competente, com a habilidade demonstrada de se organizar para atacar e comprometer computadores do governo e da indústria. [...] é um grupo ou um conjunto de grupos associados de forma livre, às vezes com interesses comuns, organizado para atingir objetivos sociais. Esses objetivos variam de comerciais (expondo detalhes embaraçosos de relações empresariais) a sociais (expondo corrupção ou interrompendo serviços governamentais, enquanto facilita e organiza a comunicação e os esforços dos cidadãos interessados) [...] O grupo realizou, com sucesso, ataques de negação de serviço contra bancos, penetrou e roubou dados confidenciais de órgãos governamentais (municipais, estaduais, federais e internacionais) e expôs informações confidenciais, causando efeitos devastadores. Essas informações incluíam as identidades de funcionários e executivos e detalhes de relações comerciais entre empresas e agências do governo (grifo nosso).

Planejamento da anatomia dos ataques

Como vimos anteriormente, o planejamento se inicia com a realização e a aplicação prática de várias análises, cujo principal objetivo é criar um perfil do alvo. Com isso, a anatomia do ataque será coerente com as informações obtidas e com o tipo de ataque a ser realizado. Na Figura 1, podemos visualizar alguns passos da anatomia de ataques passivos.

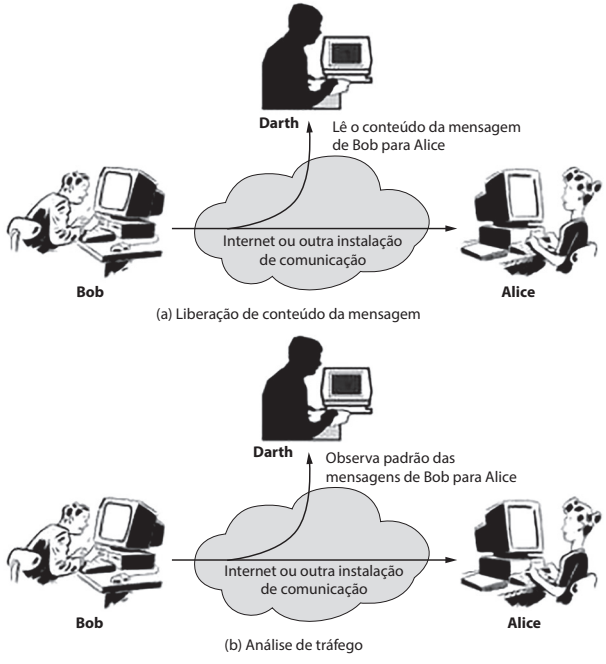

Figura 1. Anatomia de ataques passivos.
Fonte: Adaptada de Stallings (2008, p. 6).

Observe que, conforme Stallings (2008), os ataques passivos possuem a natureza de bisbilhotar ou monitorar transmissões, tendo como objetivo obter informações. Dois tipos de ataques passivos são a liberação de conteúdo da mensagem e a análise de tráfego. A liberação do conteúdo da mensagem, representada na Figura 1a, é facilmente compreendida: o invasor tem acesso a informações, que podem ser importantes ou confidenciais, transmitidas em uma conversa telefônica, uma mensagem de correio eletrônico ou um arquivo

transferido. Já na análise de tráfego, representada na Figura 1b, o invasor observa padrões de comunicação de um usuário, o que possibilita que planeje um ataque. Existem formas de "disfarçar" o conteúdo de determinadas mensagens.

Já na Figura 2, observamos alguns passos da anatomia de ataques ativos. Diferentemente dos ataques passivos, os ativos envolvem alguma modificação do fluxo de dados.

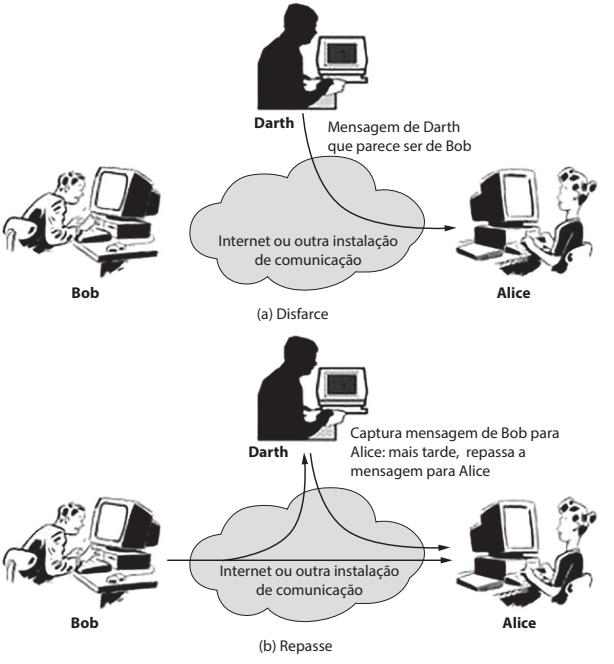

Figura 2. Anatomia de ataques ativos.
Fonte: Adaptada de Stallings (2008, p. 7).

No caso da Figura 2, temos uma situação de disfarce, que é quando uma entidade finge ser outra, como podemos observar na Figura 2a, e uma repetição, que envolve a captura passiva de uma unidade de dados e sua subsequente retransmissão, visando a produzir um efeito não autorizado, conforme demonstrado na Figura 2b, com base em Stallings (2008, p. 7).

Saiba mais

Sobre a organização de crimes cibernéticos denominada RBN, McClure, Scambray e Kurtz (2014, p. 327) dizem o seguinte:

> A Russian Business Network (RBN) é um sindicato do crime de indivíduos e empresas sediado em São Petersburgo, Rússia, mas que em 2007 tinha se espalhado para muitos países por meio de filiais, cometendo crimes eletrônicos internacionais. O sindicato opera vários botnets disponíveis para aluguel, transmite spams, phishing, distribuição de códigos maliciosos e hospeda sites pornográficos (incluindo pornografia infantil) por assinatura. Os botnets operados ou associados à RBN são organizados, têm o objetivo simples de roubo financeiro e de identidade e utilizam ferramentas de malware muito sofisticadas para permanecer persistentes nos computadores das vítimas.

Em geral, existem diversas anatomias referentes aos tipos de ataques, porém, cada ataque será desenvolvido conforme as condições pré-estabelecidas para que ocorra. Por exemplo, um ataque *cracker*, no qual uma pessoa tenta acessar sua máquina, acontece inicialmente por meio de uma varredura de vulnerabilidades; depois, ocorre a enumeração dos tipos de serviços disponíveis, e, assim, o ataque toma forma. Um passo que está sempre presente em qualquer ataque é a definição do público-alvo. Diante dessas informações, é importante termos cuidado com o que disponibilizamos na rede, evitando a exposição de informações confidenciais sem a devida proteção. Além disso, é importante conhecer os tipos de ataques, os programas maliciosos existentes e a forma como são implantados, buscando-se sempre a prevenção desses ataques a partir da proteção específica dos dispositivos e da cautela no recebimento de arquivos e dados, por quaisquer meios.

Referências

McCLURE, S.; SCAMBRAY, J.; KURTZ, G. *Hackers expostos*: segredos e soluções para a segurança de redes. 7. ed. Porto Alegre: Bookman, 2014.

STALLINGS, W. *Criptografia e segurança de redes*. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

Leituras recomendadas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR/ISO/IEC 17799*: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

FONTES, E. L. G. *Segurança da informação*: o usuário faz a diferença. São Paulo: Saraiva, 2006.

PEIXOTO, M. C. P. *Engenharia social e segurança da informação na gestão corporativa*. Rio de Janeiro: Brasport, 2006.

POLIZELLI, D. L.; OZAKI, A. M. *Sociedade da informação*: os desafios da era da colaboração e da gestão do conhecimento. São Paulo: Saraiva, 2008.

WRIGHTSON, T. *Segurança de redes sem fio*: guia do iniciante. Porto Alegre: Bookman, 2014.

Segurança em *webservices*

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Definir segurança da informação.
- Esclarecer sobre os riscos dos dados e comunicação.
- Propor soluções de segurança para tráfego e armazenamento de dados.

Introdução

Cada vez mais, há aplicações que precisam se comunicar entre si, e, à medida que se dá a inovação tecnológica, crescem os problemas de comunicação e segurança. Ter os dados de cartão de crédito espionados na hora em que o cliente os informa para uma compra em um *e-commerce* pode constituir um problema sério para uma empresa e seus clientes.

Para que consigamos propor soluções de segurança para tráfego e armazenamento de dados, é necessário conhecer os riscos dos dados e comunicação, bem como de conceitos de segurança da informação, além de protocolos, ferramentas e tecnologias passíveis de utilizar para alcançar melhores níveis de proteção dos dados.

Neste capítulo, você conhecerá a respeito da segurança da informação, dos requisitos que precisam ser atendidos para garantir a segurança em transferência de dados na *web*, dos riscos dos dados e comunicação, como Denial of Service (DoS), SQL Injection e Man-in-the-middle, bem como soluções de segurança [p. ex., criptografia, Single Sign-on e Virtual Private Network (VPN)].

1 Segurança da informação

Com o crescimento cada vez maior da quantidade de soluções tecnológicas, em razão da evolução dos dispositivos tecnológicos e dos meios de comunicação, as empresas se tornam cada vez mais dependentes da comunicação entre sistemas, aplicativos e dispositivos, os quais, entre outros benefícios, podem melhorar e automatizar seus processos internos.

De acordo com a Mega Sistemas Corporativos (2018), comumente as grandes empresas utilizam um conjunto robusto de ferramentas digitais, que se comunicam entre si. Cada ferramenta tem um propósito, como sistemas de comunicação de equipes, sistemas de gestão de tarefas, pessoas e vendas, sistemas contábeis, repositórios de código, ferramentas de testes e de atendimento ao cliente, etc.

Muitas vezes, a comunicação entre aplicações distintas se dá de maneira transparente para os usuários. Segundo Vargas (2001), em sistemas distribuídos, as soluções são formadas por dispositivos autônomos e *software* que fornecem abstração como se fossem uma única máquina. Nesse tipo de sistema, a comunicação, ou troca de mensagens, ocorre por meio dos objetos de dados, cuja estrutura e aplicação são definidas pelas soluções de *software* que os utilizarão.

De acordo com Durbano (2018), a segurança da informação dessas aplicações tem importância fundamental para as empresas, sobretudo para o setor de tecnologia da informação (TI), correspondendo ao conjunto de ações que tem como objetivo proteger um conjunto de dados e o seu valor, tanto para as pessoas quanto para as empresas. Ainda, ela se aplica a todos os aspectos de proteção de dados, e não apenas a sistemas computacionais.

Segundo Acosta (2015), os principais elementos da gestão da segurança da informação compreendem as políticas de informação e segurança da informação, a análise de riscos, os requisitos de segurança, os controles, as informações e os sistemas de informação e as ameaças e vulnerabilidades, como mostrado na Figura 1.

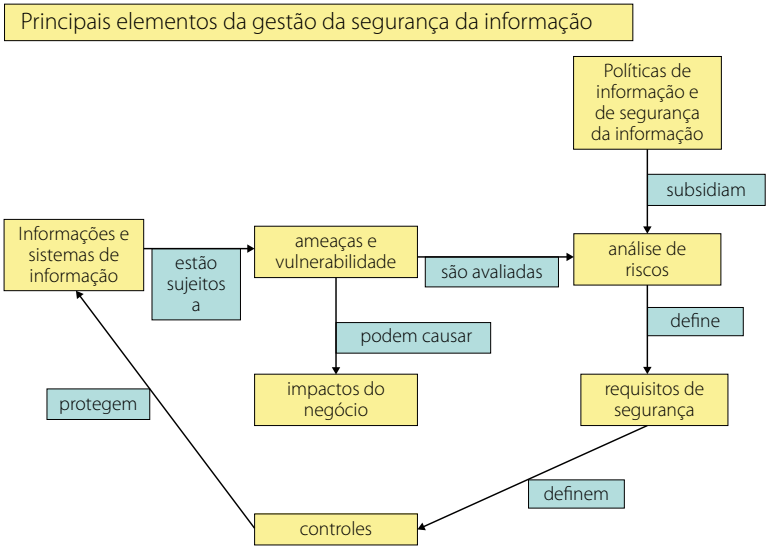

Figura 1. Principais elementos da gestão da segurança da informação e suas relações.
Fonte: Adaptada de Acosta (2015).

Para garantir a segurança das informações trocadas pela *web*, como no caso de usuários que realizam compras e fornecem informações para comércio eletrônico, quatro requisitos de segurança, listados a seguir, devem ser atendidos (GRAHAM *et al*., 2005).

- Confidencialidade — garante a proteção da informação que está sendo trocada na comunicação *web*, para que não seja exposta para outras pessoas.
- Integridade — garantia de que uma mensagem chegará da mesma maneira que foi enviada, sem ser modificada.
- Autenticação — assegura o acesso aos aplicativos e a seus dados para quem puder comprovar a sua identidade (p. ex., com *login* e senha).
- Irretratabilidade — maneira de certificar que o remetente da mensagem não possa negar o envio e que o receptor não possa negar o recebimento da mensagem.

E um quinto requisito eventualmente útil para permitir que apenas pessoas apropriadas consigam acessar os dados é a autorização, que trata da proteção de recursos, uma vez que o usuário esteja autenticado na aplicação, para que apenas as entidades apropriadas consigam acessar determinados recursos mesmo que autenticados, como no caso de informações em painéis administrativos. Assim, os sistemas podem identificar a entidade e definir se ela conseguirá acessar determinado recurso.

Segundo Wu *et al*. (2013), em virtude da definição de uma arquitetura de *webservices*, unidades de negócio, clientes e parceiros podem conseguir trocar informações, uma capacidade de comunicação vital para o sucesso dos negócios. Assim, os *webservices* possibilitam a união de informações distribuídas de forma prática e econômica, independentemente das barreiras de sistemas operacionais, da plataforma de desenvolvimento e das linguagens de programação.

De maneira simplificada, *webservices* são funções de objetos expostos via HTTP usando mensagens SOAP puras. Em termos de protocolos, um *webservice* inclui os seguintes componentes ou camadas (Figura 2): Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL) e Universal Description, Discovery and Integration (UDDI).

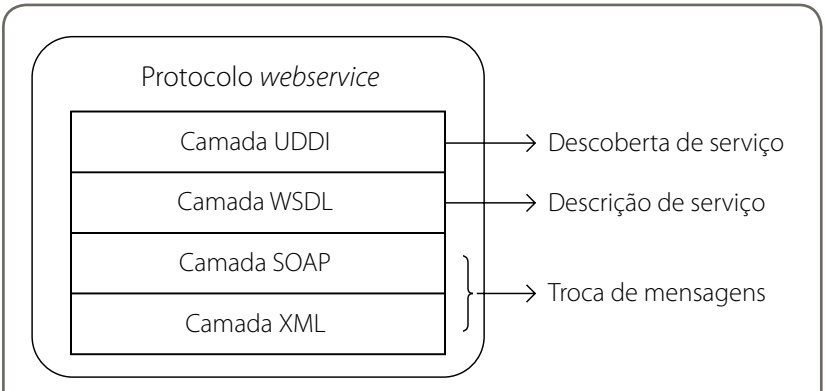

Figura 2. Protocolos usados em *webservices*.
Fonte: Adaptada de Wu *et al*. (2013).

O XML fornece um meio de troca de mensagens pela *web*, por meio de um documento que contém solicitações de informações e respostas entre sistemas diferentes. O SOAP é um padrão ou especificação de trocas de mensagens simples por documentos XML, que permite a comunicação eficaz entre remetentes e destinatários. A WSDL é responsável pela descrição completa para a comunicação entre aplicações. Já a UDDI representa uma forma de publicação e procura de *webservices* na rede, independentemente da plataforma, com registros baseados em XML.

Conforme Graham *et al*. (2005), o SOAP permite a interação mútua dos aplicativos. Para realizar a integração das aplicações entre os negócios, são utilizadas a WSDL e a UDDI. Essa integração e o uso dessas tecnologias de *webservices* possibilitam a criação de aplicações de baixo acoplamento, descentralizadas, com alcance que ultrapassa os limites das empresas. Com isso, desafios precisam ser solucionados em relação à segurança dos *webservices*.

De acordo com Wu *et al*. (2013), a segurança de *webservices* baseia-se em padrões XML abertos, aprovados pela W3C, grupo responsável por fornecer a base de segurança para aplicações que consomem *webservices*. Esses padrões independem da plataforma e promovem a interoperabilidade entre as aplicações. Além disso, a OASIS, grupo responsável por padrões abertos, publicou padrões que definem a forma de expansão de segurança para a comunicação por trocas de mensagens SOAP.

Com base nos critérios de segurança de informação apresentados, há desafios de segurança que precisam ser superados em cada um dos contextos, como apresentado a seguir.

2 Riscos dos dados e comunicação

São diversos os desafios e as complexidades relacionados aos *webservices* capazes de prejudicar os dados e a comunicação em termos de segurança (KUYORO *et al*., 2012), já que as eventuais ameaças tendem a comprometer a confidencialidade, a integridade ou a disponibilidade de um *webservice* ou do sistema *back-end* exposto por um conjunto de *webservices*, afetando apenas *webservices* ou também *sites*.

Para Durbano (2018), as aplicações de *big data* têm se tornado cada vez mais comuns nas empresas, muitas das quais se comunicam por meio de *webservices*. Entretanto, esse uso apenas faz sentido se os dados estiverem

corretos e disponíveis: quando uma falha acontece, o servidor pode parar de receber informações, podendo comprometer a análise e gerar uma predição errada para determinada situação. Além disso, empresas trabalham com informações estratégicas transmitidas pela *web* e podem ser alvo de *hackers*.

Independentemente do tipo ou do tamanho da falha, ela pode provocar problemas para os negócios. Portanto, é importante que gestores invistam em segurança da informação por meio de ferramentas e técnicas que visem a melhorar a segurança dos próprios negócios, um trabalho que, se bem-feito, pode evitar ataques digitais, falhas humanas ou desastres tecnológicos.

Quando falamos de confidencialidade, um erro é capaz de causar a exposição de dados estratégicos de uma organização ou o vazamento de dados de clientes, que podem ser capturados por *hackers*. Essa falha de segurança costuma ficar evidenciada para o público, promovendo prejuízos financeiros e problemas para a imagem da empresa.

Já o risco que diz respeito à integridade das informações está relacionado a uma falha em arquivos importantes, que podem ser corrompidos com um erro no disco rígido. Se a empresa não tiver *backup*, as operações podem ficar comprometidas.

A indisponibilidade é outro risco associado aos dados e à comunicação, tornando-se essencial que os dados estejam acessíveis no momento em que forem requisitados, especialmente quando se trata da garantia de agilidade de processos das empresas. Um dos possíveis causadores de indisponibilidade são os ataques de sequestro de dados, nos quais *hackers* solicitam valores para resgate ou para não publicá-los.

Com o objetivo de garantir a segurança de dados, também é indispensável buscar garantir a autenticidade das informações, para assegurar que o objeto não sofreu mutações ao longo do processo. Assim, evitam-se fraudes, como no caso de roubo e clonagem de informações de cartões de crédito.

De modo geral, conforme Kuyoro *et al*. (2012), as principais ameaças à segurança que podem acontecer em qualquer aplicativo *web* são relacionadas a injeção de SQL, ataques de captura e reprodução, estouros de *buffer*, ataques de negação de serviço, tratamento inadequado de erros, acessos de bisbilhoteiros e sequestros de sessão.

Segundo Durbano (2018), os crimes cibernéticos crescem a cada ano, cujos responsáveis tendem a realizar invasões com o objetivo de capturar informações dos sistemas das empresas para obter vantagem, sobretudo para vazar informações, sequestrar dados, promover ataques distribuídos de negação de serviço (DDoS) ou ataques de negação de serviço (DoS), etc.

Os DoS são realizados para comprometer a disponibilidade do sistema, por exemplo, ao consumir recursos de aplicativos na *web* para que outros usuários não consigam mais acessá-los ou mesmo utilizar o aplicativo. Esses ataques podem ser cometidos ao enviar solicitações com buscas que resultam em grandes quantidades de dados, quando os *hackers* bloqueiam as contas de usuários ou causam a falha de todo o aplicativo por meio da sobrecarga do serviço com um grande número de solicitações; normalmente, essas abordagens são combinadas com outros ataques específicos de *webservices* para maximizar os danos.

Em relação às ameaças que envolvem *webservices*, pelo fato de as instruções SQL serem criadas no decorrer da execução do sistema, dinamicamente, surge uma oportunidade de violar a segurança por meio da injeção de SQL nas mensagens. Quando *hackers* conseguem quebrar a segurança, podem transmitir entradas para a instrução SQL, para que estas façam parte da instrução.

Com essa brecha, os *hackers* podem utilizar técnicas para acessar dados privilegiados e áreas protegidas sem dispor das credenciais adequadas, além de manipular o banco de dados, o que acontece por meio da inserção de valores ou caracteres especiais nas solicitações SOAP, nos envios de formulários ou nos parâmetros das URL.

Outra ameaça, relacionada à captura e à reprodução, diz respeito aos ataques intermediários nas mensagens transmitidas pela internet, situação em que os *hackers* capturam, manipulam e reproduzem uma solicitação SOAP, modificando-a antes que chegue ao seu destino.

Ainda em relação à ameaça de captura de dados, existem riscos de invasores bisbilhoteiros interceptarem mensagens SOAP, frequentemente transmitidas por meio de *webservices*, para ler e roubar informações. As informações roubadas que mais causam prejuízo para os usuários são as senhas e as informações do cartão de crédito. Assim, é importante manter a transmissão com segurança para que essas pessoas não autorizadas não consigam interceptar as mensagens.

No caso de aplicativos nativos, *hackers* conseguem ameaçar servidores por meio de *webservices* que contenham mensagens com tamanho de dados de entrada não verificados, ataques que podem acontecer por meio de solicitações SOAP ou envio de formulários *web*. Nos ataques de estouro de *buffer*, os *hackers* especificam mais dados em campos para gravar do que o tamanho em memória disponível para retê-los. Essas funções criadas por *hackers* para acessar informações não autorizadas podem resultar em falhas no aplicativo, em comprometimento do sistema ou no início de processos não autorizados.

De acordo com Kuyoro *et al*. (2012), existem ainda ameaças relacionadas ao tratamento inadequado de erros. Diversos servidores retornam detalhes da aplicação quando acontece um erro interno, os quais são úteis para a equipe de desenvolvimento para depurar o código. Entretanto, quando o aplicativo está em produção, essas informações não devem chegar aos usuários comuns, tendo em vista que podem incluir informações do código do projeto e expor possíveis vulnerabilidades.

Um problema de segurança associado a esse tipo de ameaça se dá quando o sistema retorna uma mensagem de erro para um usuário mal-intencionado, informando que a consulta SQL está incorreta. Com isso, o usuário recebe a informação de que as entradas podem ser utilizadas para gerar consultas ao banco de dados e consegue realizar a injeção de SQL indesejado (*SQL injection*), como exemplificado na Figura 3.

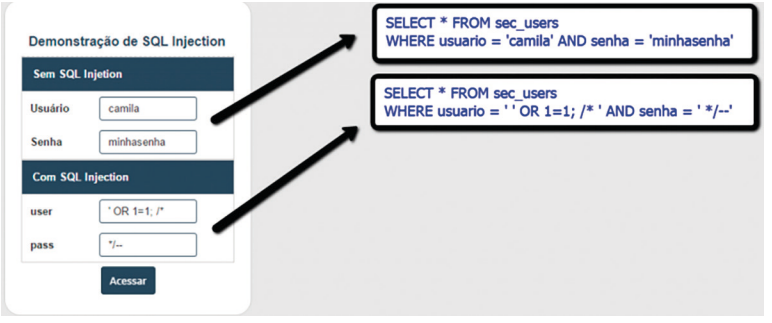

Figura 3. Exemplo de *SQL injection*.
Fonte: Moreira (2019, documento *on-line*).

Outro problema possível refere-se ao momento em que o sistema informa ao usuário que a senha está errada, situação em que o criminoso pode tentar outras senhas do mesmo usuário.

Para Durbano (2018), é importante se atentar ao cenário mundial atual e às suas necessidades de segurança, o que pode evitar graves prejuízos para as empresas e para a sociedade como um todo. Para isso, tornam-se necessários planejar e implementar medidas de segurança da informação alinhadas ao negócio de modo integral, evitando muitos dos eventuais problemas e determinando os planos de contingência que podem ser aplicados caso aconteça algo errado.

Os resultados para uma empresa que não investe em segurança podem ser desastrosos, assim como quando da utilização de soluções mais econômicas e menos eficientes ou quando algumas práticas deixam de ser implementadas. Se os dados ficarem inacessíveis para os usuários, os serviços podem ficar paralisados e o processo de correção do problema levar dias para ser solucionado.

De acordo com o serviço prestado, alguns minutos podem provocar grandes prejuízos financeiros. Além do acesso aos dados, outras fragilidades de segurança da organização são capazes de determinar a confiabilidade do mercado em relação à empresa, que pode perder os clientes por conta da exposição de dados sensíveis e sofrer processos judiciais em relação a essa falha de segurança das informações.

A seguir, mostraremos algumas propostas de soluções de segurança para tráfego e armazenamento de dados, que visam a proteger os dados das pessoas e das empresas.

3 Soluções de segurança

De acordo com Kuyoro *et al*. (2012), na década de 1990 o trabalho dos profissionais de segurança era relativamente simples, já que os dados sensíveis estavam localizados em bancos de dados monolíticos, com apenas alguns poucos caminhos de acesso aos dados, protegidos por mecanismos de controle de acesso.

Por muitos anos, utilizaram-se políticas, procedimentos e ferramentas para proteger bancos de dados legados e, com o surgimento de aplicações baseadas na *web*, especialmente em relação às aplicações de comércio eletrônico que acessam servidores na internet, a segurança se tornou ainda mais importante. Com essa evolução, surgiram tecnologias que amadureceram ao longo do tempo, como o Secure Socket Layer (SSL), os *firewalls*, a autenticação e a autorização pela *web*, que fortalecem a segurança entre os navegadores dos clientes e os servidores *web* das empresas.

O SSL, uma tecnologia ou protocolo utilizado para proteger contra ataques que invadam a segurança de *webservices*, criam um túnel seguro entre as máquinas cliente e servidor com base na técnica de criptografia de chave pública, comumente empregada para o envio seguro de mensagens. Para diversos aplicativos simples, esse tipo de tecnologia pode ser o suficiente; no caso de *webservices*, as mensagens podem ser criptografadas e assinadas para proteção da confidencialidade das informações e integridade dos dados.

Assim como o SSL, existe um conjunto de tecnologias com o objetivo de adicionar segurança aos *webservices*, como a extensão do SOAP WS-Security (WSS), que deve ser utilizada preferencialmente em conjunto com outros *webservices* e protocolos específicos de aplicações. O WSS determina como os dados de assinatura XML podem ser incluídos na mensagem SOAP: as especificações XML de assinatura e criptografia fornecem métodos-padrões para a assinatura digital e a criptografia de documentos que incluam mensagens SOAP, um processo utilizado tanto para documentos inteiros quanto para partes menores.

Outra tecnologia de segurança em *webservices* consiste na criptografia por meio de código XML, uma das maneiras de fornecer segurança de ponta a ponta para os aplicativos que exigem alteração segura dos dados, além de uma forma natural de lidar com requisitos de segurança em dados trocados entre aplicações. Esse tipo de criptografia não substitui o SSL, mas provê um mecanismo para os requisitos de segurança não cobertos pelo SSL.

Outras duas técnicas baseadas em XML são a Security Assertion Markup Language (SAML) e a eXtensible Access Controle Markup Language (XACML). A primeira compreende um protocolo para declarar informações de autenticação e autorização, além de fornecer atributos de um usuário final no formato XML e permitir adicionar informações a uma mensagem SOAP. Para possibilitar o *single sign-on* (SSO), servidores SAML podem ser acessados a fim de obter dados de autenticação e autorização, como visto na Figura 4.

Figura 4. Representação esquemática do *single sign-on*.
Fonte: Adaptada de Rodrigues (2017).

Caso o destinatário da mensagem SOAP confie no emissor dos dados SAML, o usuário também poderá ser autorizado para o *webservice*.

Já a XACML foi projetada para expressar regras de controle de acesso no formato XML.

E, mesmo que as duas técnicas não estejam explicitamente ligadas, podemos usá-las em conjunto, caso em que uma decisão de autorização expressa em uma declaração SAML pode ter sido baseada em regras expressas em XACML.

Dubin (2008) afirma que existem diversas opções de segurança baseadas em XML disponíveis quando falamos de *webservices*, as quais gerenciam criptografia, controle de acesso, autenticação, integridade e privacidade de dados necessários nos *webservices*. Para o autor, além do SAML, são outras possibilidades as assinaturas digitais em XML, o XML Key Management Specification (XKMS) e o serviço de mensagens ebXML, que não serão aprofundados neste capítulo.

Segundo Durbano (2018), aplicar as práticas de segurança não é o suficiente, exigindo-se a garantia de que não haverá brechas. Para isso, é necessário aplicar as melhores ações existente na área, o que requer um acompanhamento contínuo das tendências e das evoluções da área, possibilitando a criação de soluções de proteção para os novos mecanismos de ataque. Ainda, é preciso manter os *software* e *drivers* dos dispositivos atualizados, estabelecer o controle de acesso aos colaboradores e políticas de segurança, alinhar os processos às políticas de segurança, fazer planos de contingência e empregar ferramentas de monitoramento e criptografia dos dados.

Para Graham *et al*. (2005), as técnicas de criptografia fornecem uma base para proteção de mensagens trocadas entre parceiros. A confidencialidade e a integridade podem ser garantidas com tecnologias de criptografia e a assinatura digital, respectivamente, categorizadas entre chaves ou criptografias simétricas e assimétricas.

A criptografia simétrica exige o uso da mesma chave para o processo de criptografia e descriptografia — quando uma pessoa pretende enviar uma mensagem para outra, a mensagem é criptografada com uma chave, e, quando o destinatário a recebe, também deve ter a mesma chave para que consiga obter a mensagem original. Considerando que a mesma chave é utilizada em ambos os pontos, esse tipo de criptografia é chamado de criptografia simétrica, bem como as chaves levam em geral o nome de chaves simétricas.

A criptografia assimétrica simplifica a distribuição de chaves, tendo em vista que possibilita tornar a chave de criptografia pública. Nesse caso, utilizamos duas chaves distintas em cada uma das pontas: uma chave pública e outra chave privada. A chave pública é utilizada para criptografar a mensagem, e a única maneira de descriptografar a mensagem se dá por meio da chave privada. Pelo reflexo da sua natureza assimétrica, essas chaves são chamadas de assimétricas.

Outra técnica bastante utilizada para melhorar a segurança na troca de mensagens é a utilização de VPN, com a qual se pode criar uma rede privada sobre a infraestrutura de uma rede pública, como observado na Figura 5.

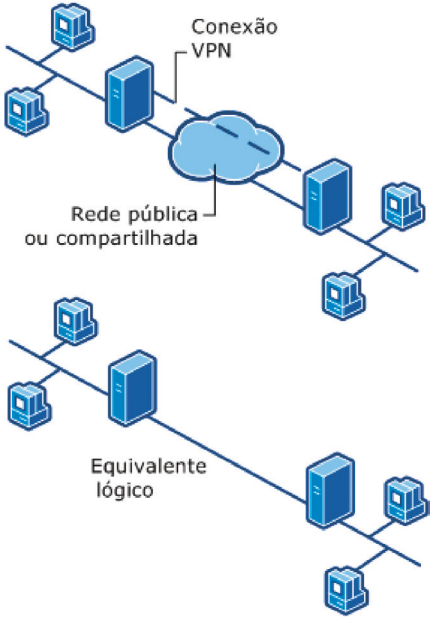

Figura 5. Exemplo de VPN.
Fonte: Adaptada de Rodrigues (2017).

Nesse tipo de rede, a criptografia nas informações e na comunicação pode aumentar a confidencialidade consideravelmente. O sistema de tunelamento permite a troca de mensagens sem que outras pessoas tenham acesso, ou que a mensagem esteja criptografada caso seja acessada.

De acordo com Cabral (2018), grandes empresas também utilizam a técnica de segmentação da rede por questões de segurança: a empresa cria compartimentos digitais e, caso uma máquina na rede ou a própria rede seja atacada, isso somente acontece no compartimento em questão, e não nos demais. Com isso, quando atacados, uma quantidade menor de dados fica exposta aos criminosos, minimizando os impactos. Além disso, também é importante proteger as redes com *firewalls* e outros mecanismos.

Neste capítulo, pudemos observar conceitos de segurança em *webservices*, além dos riscos que os dados e a comunicação sofrem, e eventuais soluções de segurança para tráfego e armazenamento de dados utilizadas para proteger os dados e a rede.

Referências

ACOSTA, I. *Segurança da informação*. 2015. Disponível em: https://slideplayer.com.br/slide/3550546/. Acesso em: 11 jun. 2020.

CABRAL, T. *Entenda a importância de segmentar a rede para mantê-la segura*. 2018. Disponível em: https://blog.athenasecurity.com.br/segmentacao-de-rede/. Acesso em: 11 jun. 2020.

DUBIN, J. *What are the risks of connecting a web service to an external system via SSL?* 2008. Disponível em: https://searchsecurity.techtarget.com/answer/What-are-the-risks-of--connecting-a-Web-service-to-an-external-system-via-SSL. Acesso em: 11 jun. 2020.

DURBANO, V. *Segurança da informação*: o que é e 12 dicas práticas para garantir. [2018]. Disponível em: https://ecoit.com.br/seguranca-da-informacao/. Acesso em: 11 jun. 2020.

GRAHAM, S. *et al. Build web services with Java*. 2nd ed. Indianapolis: Pearson Education, 2005.

KUYORO, S. O. *et al.* Security issues in web services. *International Journal of Computer Science and Network Security*, [*s. l.*], v.12, n.1, p. 23–27, 2012.

MEGA SISTEMAS CORPORATIVOS. *Conheça os principais tipos de integração de sistemas*. 2018. Disponível em: https://www.mega.com.br/blog/conheca-os-principais-tipos--de-integracao-de-sistemas-9192/. Acesso em: 11 jun. 2020.

MOREIRA, C. *SQL injection*: o que é e como funciona? 2019. Disponível em: https://camilamoreira.com.br/site/?p=626. Acesso em: 11 jun. 2020.

RODRIGUES, M. *Single Sign-On (SSO) server + laravel 5*. 2017. Disponível em: https://medium.com/laraveltips/single-sign-on-sso-server-laravel-5-6c7c70858c63. Acesso em: 11 jun. 2020.

VARGAS, P. K. *Comunicação em sistemas distribuídos*. 2001. Disponível em: https://www.cin.ufpe.br/~avmm/arquivos/provas%20software/resuminho2.pdf. Acesso em: 11 jun. 2020.

WU, J. *et al.* A cross-layer security scheme of web-services-based communications for IEEE 1451 sensor and actuator networks. *International Journal of Distributed Sensor Networks*, [*s. l.*], v. 9, n. 3, p. 1–10, 2013.

Leituras recomendadas

MCLAUGHLIN, B. *Java & XML*. 2nd ed. Sebastopol: O'Reilly, 2001.

ORACLE. *Fusion middleware security and administrator's guide for web services*. 2020. Disponível em: https://docs.oracle.com/cd/E17904_01/web.1111/b32511/intro_ws.htm#WSSEC2935. Acesso em: 11 jun. 2020.

VARGAS, P. K. *Sistemas operacionais distribuídos e de redes*. 2000. Disponível em: https://www.cin.ufpe.br/~avmm/arquivos/provas%20software/attachment.pdf. Acesso em: 11 jun. 2020.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Tipos comuns de invasão

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Descrever os tipos comuns de invasão e as principais técnicas usadas.
- Reconhecer os tipos de ataques de negação de serviço.
- Identificar os ataques na *web* (clientes e servidores).

Introdução

O uso de serviços na *web* vem crescendo de maneira abrangente, com ataques surgindo, por consequência, a todo momento. Com frequência, são observadas falhas nas aplicações *web*, como a vulnerabilidade das páginas, servidores e transição de dados a bancos de dados. Por isso, tornam-se necessários profissionais que conheçam o que está acontecendo no mundo cibernético.

Neste capítulo, você conhecerá sobre os tipos comuns de invasão, como as invasões *web* de clientes e servidores, as negações de serviços e as principais técnicas utilizadas por invasores.

Invasões comuns e principais técnicas

Os tipos de ataques mais comuns utilizados por invasores são citados a seguir.

DDoS Attack*, sigla de *Distributed Denial-of-Service, é conhecido como "ataque de navegação de serviço" (Figura 1), uma maneira relativamente simples de derrubar um serviço. Seu objetivo consiste em tornar uma página ou um processo indisponível para o usuário final. Para realizar esse ataque, o invasor precisa criar uma rede zumbi (BotNet), que inclui uma infinidade de computadores infectados de maneira que um *host* "mestre" possa controlar. No momento em que o *cracker* escolhe seu alvo, ele envia o IP para o computador "mestre", que se encarrega de distribui-lo para a rede de computadores "zumbis". Essa rede será responsável por sobrecarregar o alvo (p. ex., um servidor) até que se torne indisponível.

Em geral, os invasores empregam a obstrução da mídia de comunicação entre os utilizadores e o sistema de modo a não se comunicarem corretamente. Outra maneira de realizar o ataque consiste em forçar a vítima a reinicializar ou consumir todos os recursos de memória, processamento ou de outro *hardware* a fim de deixá-lo impossibilitado de fornecer o serviço. Por ter múltiplas fontes, o rastreamento e o bloqueio desse tipo de ataque são mais complicados.

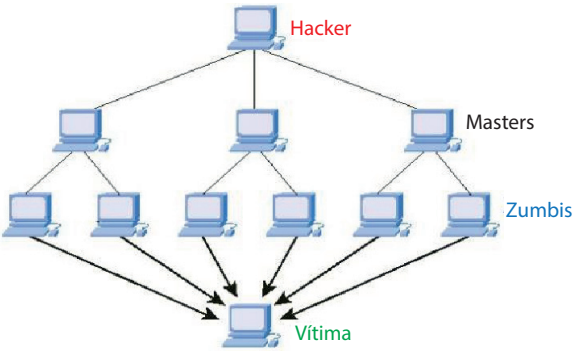

Figura 1. Exemplo ilustrativo de como acontece o ataque de DDoS na rede.
Fonte: CanalTech (2018, documento on-line).

Port Scanning Attack compreende uma técnica muito empregada pelos responsáveis pela segurança da informação, com a finalidade de encontrar fraquezas em um servidor ou vulnerabilidades no sistema. Normalmente, está relacionado ao uso de *softwares* maliciosos para que explorar as brechas dos sistemas.

Esse ataque consiste em enviar mensagens para uma porta e esperar por uma resposta. O dado ou informação recebidos indicam ao *hacker* se aquela porta está disponível ou não, o que o ajudará a encontrar a melhor maneira de invadir o servidor.

Cavalos de Troia, vírus e *malwares* são programas maliciosos desenvolvidos por invasores com o objetivo de destruir o alvo. Os vírus e *worms* (programa autorreplicante que pode ser projetado para realizar ações maliciosas após infestar um sistema e, inclusive, deletar arquivos) normalmente se aderem a um sistema de modo a inviabilizar o uso de uma máquina ou de uma rede como um todo. Normalmente, esse ataque se inicia por e-mail ou os programas ficam escondidos dentro de aplicações de interesse do usuário.

Os cavalos de Troia são parecidos — infectam o computador da mesma maneira, mas normalmente oferecem ao *hacker* acesso ao computador vitimado, passando diversos tipos de informações.

Algumas ações mais comuns do cavalo de Troia:

- criar portas dos fundos — normalmente alteram o sistema de segurança de modo que outros *malwares*, ou *crackers*, consigam invadir;
- espionar — alguns cavalos de Troia são *spyware* (programa automático de computador que recolhe informações sobre o usuário), projetados para aguardar até que o usuário acesse contas on-line ou insira dados de cartão de crédito. Depois, enviam suas senhas e dados pessoais de volta ao computador "mestre" (de onde veio o ataque);
- transformar computadores em zumbis — nesse caso, o interesse do invasor consiste em fazer o seu computador virar um escravo em uma rede sob seu controle.

Ataques de força bruta tentam adivinhar usuários e senhas por meio de tentativa e erro. Se o invasor souber o nome do usuário, apenas precisará descobrir a senha deste. Na internet, existe até mesmo um dicionário de senhas mais comuns entre os usuários.

Eavesdropping é um ataque que se baseia na violação da confidencialidade de informações e dados: o invasor, por meio de recursos tecnológicos, aproveita a vulnerabilidade nas comunicações de possíveis vítimas fazendo um monitoramento sem autorização durante essa comunicação, podendo roubar dados e informações a ser usadas posteriormente.

Esse tipo de ataque se aproveita de conexões não encriptadas, ou encriptadas, usando algoritmos fracos. Redes locais, baseadas em *hubs* ou redes *wireless*, sem segurança, são alvos fáceis, bastando plugar o *notebook* no *hub* ou colocá-lo dentro da área de alcance do ponto de acesso para capturar as transmissões.

O ***spoofing*** é um ataque no qual o invasor se passa por outro aparelho ou usuário de uma rede. Tem os objetivos de roubar dados, disseminar *malwares* ou contornar controles de acesso. Suas formas mais comuns são o *spoofing* de IP, e-mail e DNS. O *spoofing* tenta enganar uma rede ou uma pessoa fazendo-a acreditar que a fonte de uma informação é confiável.

Exemplo

Um invasor pode realizar o *spoofing* de *e-mail* enviando a você — usuário — uma mensagem que pareça se originar de alguém ou empresa em quem ou em que confia: isso fará com que informe dados sigilosos.

Nesse caso, temos a técnica de *phishing*, na qual os dados são pescados por um relapso do usuário.

O ***bluejacking*** envia imagens, mensagens de texto e sons aos dispositivos próximos via Bluetooth. Além de invadir a privacidade de quem utiliza os aparelhos, o programa encaminha *spam*.

O ***adware*** é um modelo de *software* de invasão de privacidade, que exibe anúncios na tela de um usuário sem o seu consentimento. Em geral, é instalado no computador de um usuário porque ele visitou uma página infectada, abriu um anexo de *e-mail* infectado, instalou um programa que tinha *adware* embutido em um cavalo de Troia ou surge como resultado de um vírus ou um verme de computador. Quando estiver instalado e executando em segundo plano, um programa *adware* periodicamente exibirá um anúncio na tela do usuário.

O ***spyware*** é um *software* de invasão de privacidade instalado em um computador de usuário sem sua autorização, coletando informações sobre ele. Normalmente, a infecção do *spyware* envolverá outros programas, que sempre estarão em execução em segundo plano, consumindo a memória e o processamento do seu computador. Muitas vezes, uma infecção com esse tipo de *software* pode modificar o sistema operacional de modo que o *spyware* seja sempre executado como parte da sequência de inicialização do sistema. O computador infectado normalmente trabalha em modo de lentidão.

Vejamos algumas das diferentes ações executadas por um *spyware*.

- Captura de teclas: também conhecida como *keylogging*, refere-se ao monitoramento das ações de uma tecla de computador registrando cada tecla pressionada. Normalmente, tem a intenção de resgatar senhas, informações de *login* e outras informações confidenciais, como o número de cartão de crédito. Esse tipo de interceptação pode funcionar capturando cada tecla pressionada, retornada pelo *hardware* e gravando-a em um local oculto, antes de passar as informações obtidas para o sistema operacional.

- Captura de tela: capturar uma tela de usuário pode revelar uma grande quantidade de informações. Uma infecção de *spyware*, que usa capturas periódicas de telas, pode comprometer a privacidade do usuário. Um *spyware*, que se mantém anônimo no sistema operacional, deve fazer capturas de tela a uma taxa relativamente baixa do uso da memória.
- Rastreamento de *cookies*: *cookies* são arquivos de internet que armazenam temporariamente aquio que o internauta está visitando na rede. Eles fornecem uma maneira de *sites* manterem o estrado entre várias visitas do mesmo usuário, como um modelo de lembrete, e proporcionam uma experiência de navegação personalizada. Quando o internauta visita um *site* pela primeira vez, este pode solicitar um arquivo, denominado *cookie*, para que seja colocado em seu computador a fim de armazenar as informações úteis sobre as páginas acessadas. Infelizmente, um grupo de *sites* pode agir de maneira maliciosa e solicitar que *cookies* de determinada nomenclatura e tipo sejam instalados, de modo a poder a fazer um rastreamento coletivo quando um usuário visitar qualquer um de seus *sites. Cookies* utilizados como no exemplo são visualizados como um tipo de *spyware*, mesmo que não exista um *software* instalado no computador do usuário.

Exemplo

Um exemplo de utilização de *cookies* rastreadores são as empresas de publicidade. Aquelas com anúncios em diversas páginas da *web* empregam esse sistema para identificar quais de seus *sites* clientes foram visitados por um usuário em particular.

- Coleta de dados: esse tipo de *spyware* evita problemas e riscos associados ao monitoramento de ações do usuário. Sua intenção é procurar dados pessoais ou proprietários nos arquivos de computadores infectados.

Exemplo

Dois exemplos que se pode citar para a coleta de dados são:

- inclusão de programas que procuram uma lista de contatos do usuário para coletar endereços de *e-mails* que possam ser utilizados para *spams*;
- programas que procuram documentos, planilhas e apresentações de slides capazes de conter dados de interesse do desenvolvedor do *spyware*.

Fique atento

Você já ouviu falar nas **zonas cinzas**? Zonas cinzas envolvem a instalação de *spywares* bem-intencionados, pois estão em uma zona ética, usados de forma consciente — ou seja, eles têm a intenção de monitorar o que está sendo acessado nos computadores, como o caso de pais que monitoram o uso de computadores de seus filhos. Trata-se de um tipo de sistema voltado a manter segurança em relação aos acessos de uma máquina.

Ataques de negação de serviços

Identificados como *Denial-of-Service Attack* (DoS), esses ataques fazem com que recursos sejam explorados de modo que usuários legítimos fiquem impossibilitados de utilizá-los. Em outras palavras, qualquer ataque planejado para fazer uma máquina ou um *software* ficar indisponível e incapaz de executar sua funcionalidade básica é conhecido como ataque de negação de serviço.

Nesse tipo, a falsificação do endereço IP de origem é comumente usada para obscurecer a identidade do atacante. O uso de falsificação de IP dificulta a identificação da fonte de um ataque DoS.

Ataque ICMP (*Internet Control Message Protocol*)

Existem dois ataques de negação de serviço que exploram ICMP:

- **ataque de inundação por *ping*** — o utilitário ping envia uma requisição de *echo* ICMP para um *host*, que, por sua vez, responde com um *echo* ICMP. Para considerar esse ataque, uma máquina, considerada potente, envia uma quantidade grande de requisição de *echo* para um único servidor vítima. Se o atacante conseguir criar mais requisições *ping* do que a vítima pode processar, então o servidor atacado ficará sobrecarregado pelo tráfego e começará a descartar conexões legítimas;
- ***smurf*** — trata-se de um ataque no nível de rede no qual um grande tráfego de pacotes é enviado para o endereço IP (*Internet Protocol*) de *broadcast* (método de transferência de mensagem para todos os receptores simultaneamente) da rede, tendo como origem o endereço de origem da vítima. Caso o número de máquinas na rede que recebem e respondem aos pacotes enviados seja extenso, o computador da vítima será infestado com o tráfego. Isso pode atrapalhar o computador da vítima, impossibilitando trabalhar nele.

Outros ataques de negação de serviço

O Fragle utiliza pacotes UDP *echo* (*User Datagram Protocol*) em vez de ICMP *echo* (*Internet Control Message Protocol*). As máquinas na rede, ao receberem o pacote UDP, respondem à vítima, que, por sua vez, envia mais uma resposta, gerando uma grande quantidade de tráfego na rede.

Já o ***SYN Flooding*** corresponde a um ataque que explora o mecanismo de estabelecimento de conexões TCP (*Transmission Control Protocol*, ou Protocolo de Controle de Transmissão). Os ataques relacionados ao *SYN flooding* (Figura 2) se caracterizam pelo envio de um grande número de requisições de conexão, fazendo com que o servidor não consiga responder a todas elas. Nesse caso, a pilha de memória sofre uma sobrecarga e as requisições de conexões de usuários são desprezadas.

O ataque se dá quando o cliente tenta começar uma conexão TCP com um servidor, que passam a trocar uma série de mensagens entre si normalmente assim:

- o cliente requisita uma conexão enviando um SYN (*synchronize*) ao servidor;
- o servidor confirma essa requisição mandando um SYN-ACK (reconhecimento de sincronização) de volta ao cliente.
- o cliente, por sua vez, responde com um reconhecimento, e a conexão está estabelecida.

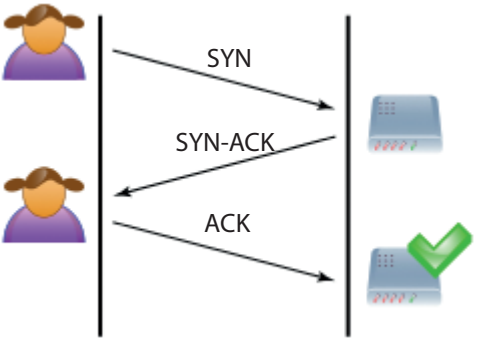

Figura 2. Exemplo ilustrativo de como acontece o ataque do *SYN Flooding*.
Fonte: TCP (2012, documento on-line).

No **ataque otimista ACK TCP,** o número de pacotes TCP como pendentes, durante uma sessão de comunicação TCP, antes de requisitar um ACK, é conhecido como janela de congestionamento. À medida que um servidor recebe ACK de um cliente, ele ajusta dinamicamente o tamanho da janela de congestionamento para refletir a estimativa de largura de banda disponível. Nesse ataque, o mecanismo de congestionamento de TCP funciona contra ele mesmo. Um pretenso cliente tenta fazer um servidor aumentar a sua taxa de envio até que esgote a sua largura de banda e não consiga atender mais ninguém com eficiência. Caso seja realizado simultaneamente contra vários servidores, esse ataque pode também criar um congestionamento na internet entre as vítimas e o atacante. Ele é feito pelo cliente que envia ACK para pacotes ainda não recebidos para fazer o servidor aumentar sua velocidade de transmissão. A intenção do cliente consiste em fazer o reconhecimento de pacotes que tenham sido enviados pelo servidor, mas ainda não recebidos pelo cliente.

Negação de serviço distribuída

A maioria dos ataques de negação de serviço é impraticável a partir de uma única máquina. As condições de negação de serviço ainda podem ser criadas usando mais de uma máquina atacante, a que se dá o nome de ataque de negação de serviço distribuída (Figura 3). Nesse tipo de ataque, invasores combinam a potência de muitas máquinas para direcionar o tráfego contra um único *site*, em uma tentativa de criar condições de negação de serviço.

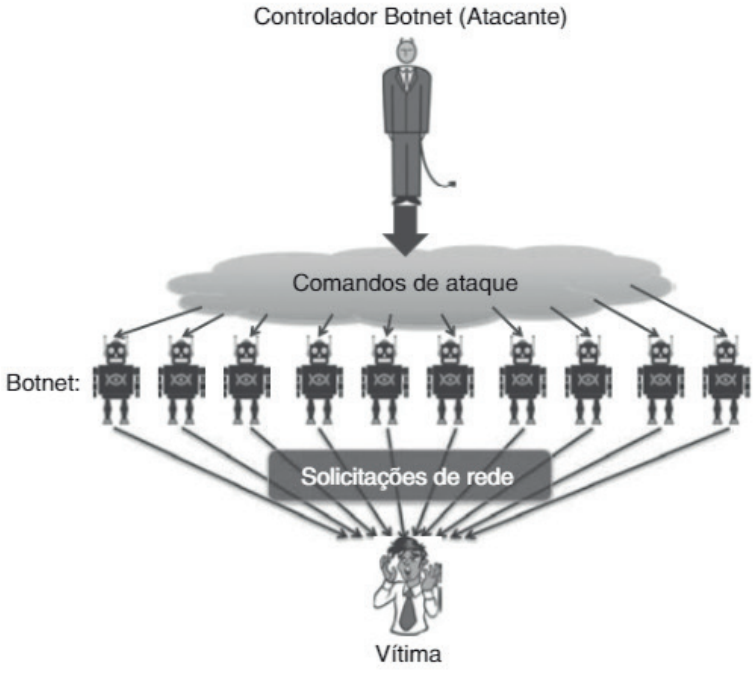

Figura 3. Exemplo ilustrativo de como acontece o ataque de negação de serviço distribuída.
Fonte: Goodrich,e Tamassia (2013).

Saiba mais

Sites como Yahoo!, Amazon e Google têm sido alvos de repetidos ataques DDOS. Com frequência, os atacantes conduzem ataques de negação de serviço usando *botnets* — grandes redes de máquinas comprometidas e que são controláveis remotamente.

Bugs em serviços e sistemas operacionais

Infelizmente, alguns dos maiores responsáveis por ataques de negação de serviços são os desenvolvedores de sistemas. Falhas na implementação e

na concepção de serviços, aplicativos, protocolos e sistemas operacionais viabilizam sua exploração em ataques contra a organização.

Vejamos alguns *bugs* e condições de *softwares* que têm como resultado a negação de serviço:

- ***buffer overflow*** — condições de *buffer* podem ser usadas para executar códigos arbitrários nos sistemas, considerados de alto risco. É preciso saber que grande parte das vulnerabilidades encontradas nos sistemas refere-se a um *buffer overflow*. Nesse tipo de ataque, o invasor explora *bugs* de implementação nos quais o controle da memória temporária para armazenamento dos dados não tenha sido feito adequadamente;

Saiba mais

O *site* de leilões online eBay foi invadido em março de 1999 pela exploração de uma condição de *buffer overflow*, em um programa com SUID *root*. O *hacker* instalou um *backdoor* que interceptava a digitação do administrador, possibilitando que nomes de acesso e senhas fossem facilmente capturados. Com um acesso de superusuário, o invasor pôde realizar várias operações no site, como modificar preços dos produtos em leilão, manipular ofertas, etc.

- condições inesperadas — manipulação errada e incompleta de entradas por meio de diferentes camadas de códigos Perl script, que recebem parâmetros pela *web* e, se forem explorados, podem fazer com que o sistema operacional execute comandos específicos;
- entradas não manipuladas — código que não define o que fazer com entradas inválidas e estranhas;
- *format string attack* — ataque a uma aplicação, em que se explora a semântica dos dados, fazendo com que sequências de caracteres nos dados fornecidos sejam processadas de modo a realizar ações não previstas ou permitidas, no âmbito do processo do servidor;
- *race conditions* — quando mais de um processo tenta acessar os mesmos dados ao mesmo tempo, podendo causar confusões e inconsistências das informações.

Fragmentação de pacotes de IP

A fragmentação de pacotes está relacionada à Maximum Transfer Unit (MTU), que especifica a quantidade máxima de dados que podem passar em um pacote por meio físico da rede.

A possibilidade de invasões por meio de fragmentação de pacotes de IP resulta do modo como a fragmentação e o reagrupamento são implementados: os sistemas não tentam processar o pacote até que os fragmentos, em totalidade, sejam recebidos e reagrupados. Isso possibilita a ocorrência de *overflow* na pilha TCP, quando há o reagrupamento de pacotes maiores que o permitido.

Ataques na *web* (clientes e servidores)

A internet é utilizada para inúmeras atividades, como serviços bancários, compras, educação, comunicação, notícias, entretenimento, redes sociais, etc. Pelo fato de ter grande acesso e estar em constante ascensão, há uma preocupação com a segurança das informações e a privacidade na *web*.

As páginas *web* utilizam o *Hypertext Markup Language* (HTML), ou seja, são escritas (desenvolvidas) pela "Linguagem de Marcação de Hipertexto". Para acessarmos um *site*, utilizamos um navegador, como Mozila Firefox, Google Chrome, Opera, entre outros, que são interpretadores, isto é, identificam um *site* com um *uniform resource locator* (URL).

Exemplo

URL corresponde aos endereços que utilizamos para acessar determinado site. Por exemplo,

http://www.exemplo.com/paginas/arquivo.html

Desmembrando o endereço, temos:

- **http** — protocolo de acesso a uma página (existem outros, como https e ftp);
- **www.exemplo.com** — domínio do servidor web, que contém o site de interesse;
- **página** — nome da pasta que está armazenando o site de interesse;
- **arquivo.html** — arquivo que descreve os textos e as imagens para uma página no site desejado.

A URL, conhecida amigavelmente por um conjunto de palavras pelos usuários da internet, transforma-se em um DNS, ou seja, o endereço que escrevemos na barra de endereços de um navegador é traduzido para um número que o identifica, com a finalidade de que a requisição aconteça de forma rápida ao servidor. Para termos um bom entendimento sobre DNS, a base será o número 128.34.66.120, o qual será requisitado ao servidor para que uma página retorne visualmente ao usuário.

Após estabelecer uma conexão TCP (Protocolo de Controle de Transmissão) com o servidor, o navegador envia requisições, conhecidas como requisição HTTP (Protocolo de Transferência de Hipertexto), para o servidor (Figura 4). Uma requisição HTTP especifica o arquivo que o navegador quer receber do servidor. As requisições ao servidor consistem em um comando GET ou POST.

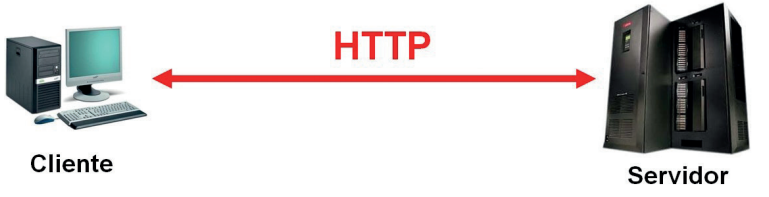

Figura 4. Requisição entre cliente e servidor.
Fonte: Padilha (2015, documento on-line).

Formulários HTML — existem para que um usuário consiga entrar em contato com determinada empresa pela internet, podendo usar dois métodos para submeter dados: GET e POST.

Quando usuários enviam os campos do formulário preenchidos e o código utilizado internamente na página HTML é o GET, os dados informados são codificados diretamente para URL, separados por "&", como em http://www.exemplo.com/form.php?nome=Teste&sobrenome=Teste de TI, no qual nome e sobrenome compreendem os campos preenchidos com as variáveis "Teste" e "Teste TI". Essa URL envia os campos preenchidos no formulário para o servidor. GET é recomendado para operações como consultas em bancos de dados que não tenham resultados permanentes.

Na submissão de dados via POST, as variáveis submetidas são incluídas no corpo da requisição HTTP, e não via URL. Esse tipo de submissão é considerado mais seguro. O POST é indicado para um processamento no qual o formulário deve inserir um registro em um banco de dados ou no envio de e-mail.

Falta de confidencialidade de HTTP — por padrão, requisições e respostas HTTP são enviadas via TCP para a porta 80, considerada uma porta-padrão. Esse protocolo não fornece nenhum meio de encriptar seus dados, ou seja, os conteúdos são enviados de forma "pura". Por essa falha na segurança (não conter encriptação), se um atacante conseguir interceptar os pacotes que estão sendo enviados pelo navegador do cliente, poderá ter acesso a qualquer informação que o usuário esteja transmitindo e, inclusive, modificá-la.

Protocolo HTTPS — para resolver problemas de confidencialidade referentes ao Protocolo HTTP, existe o HTTPS ("Protocolo de Transferência de Hipertexto Seguro") (Figura 5), que tem a mesma sistemática do HTTP, porém incorpora uma camada adicional de segurança, conhecida como SSL (*Secure Socket Layer*) ou TLS (*Transport Layer Security*). Ambos utilizam um certificado para verificar a identidade do servidor e estabelecer um canal de comunicação encriptada entre o navegador e o servidor.

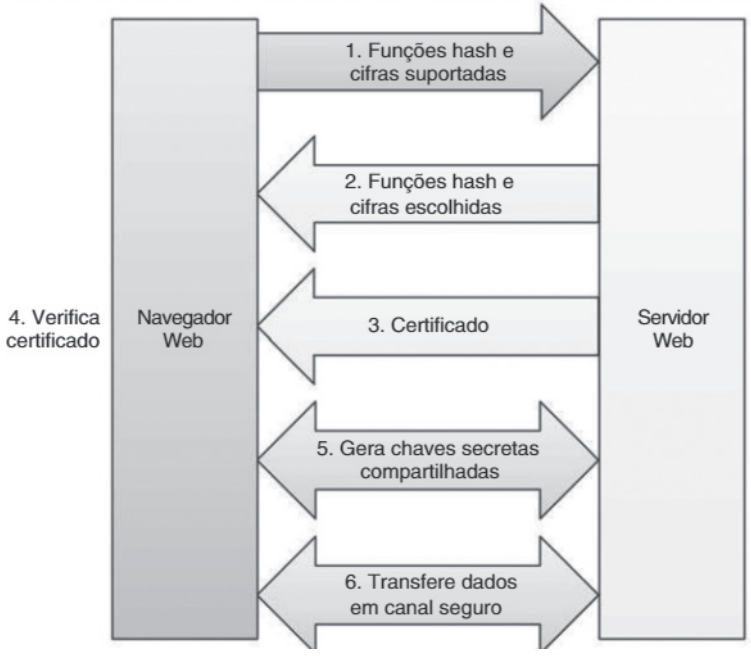

Figura 5. Como acontece uma requisição entre cliente e servidor via protocolo HTTPS.
Fonte: Goodrich e Tamassia (2013).

Certificados de servidores *web* — fornecem uma chave pública do servidor para uso na geração de chaves secretas compartilhadas, como um meio de verificar a identidade de um *site* para seus clientes. Para atingir esse objetivo, certificados são assinados digitalmente usando a chave privativa de um terceiro confiável, conhecido como Autoridade de Certificação (CA, do inglês *Certification Authority*). O proprietário de um *site* obtém um certificado submetendo uma requisição de assinatura de certificado para uma CA e pagando uma taxa.

Um certificado de servidor é um atestado do emissor (CA) sobre determinada organização, proprietária do *site*, e contém vários campos, como: nome da Autoridade de Certificação, que emitiu o certificado; número serial, identificador; data de vencimento do certificado; nome de domínio do site; organização que opera; identificador do criptossistema de chave pública usado no servidor; chave pública usada pelo servidor no protocolo HTTPS; identificador da função *hash* de chave pública usada pela CA para assinar o certificado; assinatura digital em todos os outros campos do certificado (Figura 6).

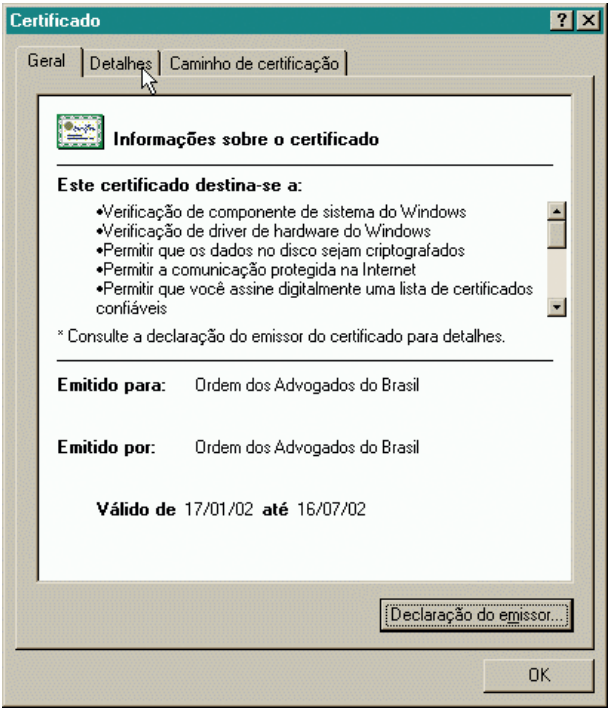

Figura 6. Visualização de um certificado digital.

Fonte: OAB (2018, documento on-line).

Quando um certificado se torna inválido, a CA o revoga, adicionando seu número serial à lista de revogação de certificado, assinada pela CA e publicada no *site* de revogação. Verificar a validade de um certificado envolve não somente a assinatura no certificado, mas também baixar a lista de revogação de certificado, analisando a assinatura nessa lista e conferindo se o número serial do certificado aparece nessa lista.

A maioria dos navegadores exibe um aviso visual ao estabelecer uma conexão segura, como um ícone de cadeado. Quando um usuário navega em um *site* que tenta estabelecer uma conexão HTTP, mas fornece um certificado expirado, revogado ou inválido, a maioria dos navegadores exibe essa informação e avisa o usuário (Figura 7).

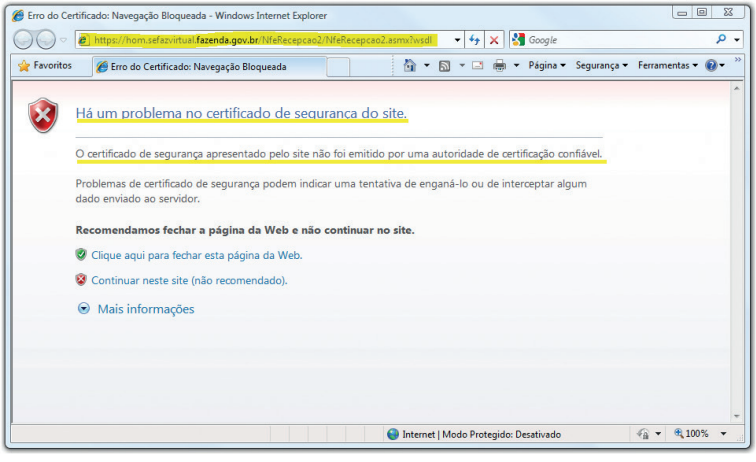

Figura 7. Aviso de certificado inválido.
Fonte: FlexDocs (2018, documento on-line).

Sessões — uma sessão encapsula informações sobre um visitante que persiste além da carga de uma única página, ou seja, um *site* com características de contas e carrinho de compras deve manter o registro de seus visitantes de modo que não se torne necessária a autenticação a cada nova página ou o registro dos números dos itens para posterior inserção em um formulário de pedidos.

A informação de sessão deve ser considerada sensível, pois é usada para permitir que os usuários mantenham uma identidade consistente em *sites* que possibilitem acessar contas bancárias, números de cartões de crédito, registro de plano de saúde, CPF, etc. O acompanhamento de uma sessão é considerado

um ataque de sequestro de sessão, no qual o invasor poderá ter acesso a todas as informações fornecidas a determinado *site*.

***Cookies* —** são enviados aos clientes pelo servidor *web* e armazenados na máquina do usuário. Quando o usuário visita o *site*, esses *cookies* retornam, inalterados, para o servidor, que pode "relembrá-lo" e acessar sua informação de sessão. *Cookies* são transmitidos, normalmente, sem encriptação, usando HTTP, e, como tal, ficam sujeitos a ataques. Para remediar a visualização de dados por meio de *cookies* pode ser configurado um sinalizador de segurança que requer a transmissão de um *cookie* usando HTTPS.

Ataques a clientes

Navegadores *web* são alvos populares de ataques, como os descritos a seguir.

Sequestro de sessão — trata-se de um sinônimo de uma sessão roubada, na qual um invasor intercepta e assume uma sessão legitimamente estabelecida entre um usuário e um *host*, a qual se dá pelo acesso de qualquer recurso autenticado, como um servidor *web*. Nesse tipo de ataque, os invasores se colocam entre o usuário e o *host*, permitindo o monitoramento do tráfego do usuário e o lançamento de ataques específicos. Sendo bem-sucedido no sequestro de sessão, o atacante pode assumir o papel do usuário legítimo ou monitorar o tráfego para injetar ou coletar pacotes específicos a fim de criar o efeito desejado. Com esse ataque, pode-se enviar comandos, roubar identidades e elevar a corrupção de dados. Podemos citar três técnicas de sequestro de sessões:

- **forçar um ID —** o invasor, que geralmente tem algum conhecimento do intervalo de ID disponíveis, adivinha um ID. O atacante pode ser auxiliado pelo uso de referências HTTP, *sniffing, cross-site scripting ou malware*;
- **roubar um ID —** um invasor roubará um ID usando *sniffing* ou outros meios;
- **calcular um ID —** um invasor tentará calcular um ID de sessão válido simplesmente olhando para um existente e, depois, descobrindo a sequência.

***Phishing* —** roubo de identidade em que o fraudador utiliza um *e-mail* que parece autêntico de uma empresa legítima ou, então, um *site* falsificado para induzir destinatários a fornecerem informações pessoais confidenciais, como o número do cartão de crédito. A maioria dos ataques de *phishing* tem como alvo empresas de serviços financeiros, mais provavelmente pelo alto valor da

informação "pescada". Uma técnica usada pelos atacantes, conhecidos como *phishers*, consiste em, de algum modo, disfarçar o URL do *site* falso para não alertar a vítima sobre algo que possa estar errado.

Sequestro de clique — exploração de um *site* no qual um clique em uma página é usado de uma maneira que não era a pretendida pelo usuário (p. ex., o usuário clica para assistir a um vídeo, mas, em vez de iniciá-lo, redireciona para outra página, indesejada). O sequestro de clique pode ser usado para forçar os usuários a clicarem nos anúncios sem desejarem, aumentando o lucro dos *sites* fraudulentos, ação conhecida como fraude do clique.

Vulnerabilidades em conteúdo — podem estar presentes em um conteúdo dinâmico de mídia. Ocorrem em virtude de ações maliciosas por parte de exibidores de conteúdo de mídia e ferramentas interativas que poderiam estar fornecendo uma experiência segura e agradável ao usuário.

***Cross-site Scripting* (XSS) —** são ataques nos quais a validação inadequada da entrada em um *site* permite que usuários maliciosos injetem um código no site, posteriormente executado no navegador de um visitante. São dois os tipos de ataques XSS:

- XSS persistente — o código que o atacante injeta no site permanece no site por um período, sendo visível para outros usuários;
- XSS não persistente — não permite que o código injetado persista após a sessão do atacante. Um exemplo refere-se à página de busca de determinado *site*, que retorna uma consulta; ao ser digitada uma pesquisa, como "informática", a página resultante iniciará com uma linha que diga "Resultados da busca sobre informática". Caso a entrada do usuário não seja filtrada para certos caracteres, a injeção de segmentos de código na caixa de pesquisa poderia resultar na inclusão de código na página de resultados de pesquisa, como conteúdo da página, executando como código no navegador do cliente.

***Cross-site request forgery* (CSRF) —** também conhecido como requisição forjada de sites, é essencialmente oposto ao XSS. Explora a confiança de um *site* em relação a um usuário específico. Nesse ataque, um *site* malicioso faz o usuário executar, sem saber, comandos em um terceiro *site*, no qual o usuário confia.

Ataques a servidores

São diários os ataques à tecnologia *web*. A partir de agora, exploraremos um pouco sobre *scripts* e alguns ataques a servidores.

***Scripts* de servidores —** o código dos servidores é executado no servidor, motivo pelo qual somente é visível ao cliente o resultado da exibição desse código, e não seu código-fonte. Em geral, o código do servidor executa operações e, eventualmente, gera um código HTML-padrão, que será enviado como resposta a uma requisição do cliente.

O PHP é uma linguagem de hipertexto de pré-processamento, que possibilita que servidores *web* usem *scripts* para criar, de maneira imediata e dinâmica, arquivos HTML para usuários com base em diversos fatores, como hora do dia, entradas fornecidas pelo usuário ou consultas em bancos de dados. O código PHP é embutido em um arquivo PHP ou HTML e armazenado em um servidor *web*, que o executa por meio de um módulo de pré-processamento PHP no *software* do servidor WEB para criar um arquivo de saída HTML enviado a um usuário.

Vulnerabilidades de inclusão de *script* no servidor — um *script* é incluído no servidor de forma vulnerável, o que é explorado por um atacante para injetar um código de *script* arbitrário no servidor, que o executa para realizar uma ação desejada pelo invasor. Compreendem alguns tipos de inclusão de arquivos:

- inclusão de arquivo remoto (RFI) — tem se tornado menos comum, pois a maioria das instalações PHP não permite, por padrão, que o servidor execute um código hospedado em um servidor separado. Esse tipo de ataque acontece a partir da verificação da necessidade de que o código do servidor execute um código externo, contido em outros arquivos, além daquele que está sendo executado naquele momento;

Exemplo

Um exemplo prático de inclusão de arquivo remoto consiste na inclusão de um cabeçalho e um rodapé comum a todas as páginas de um *site*.

- inclusão de arquivo local (LFI) — faz o servidor executar um código injetado que, de outro modo, não seria executado (normalmente para um propósito malicioso). A diferença entre a LFI e a RFI reside no fato de que o código executado não está contido em um servidor remoto, mas no próprio servidor da vítima;

Exemplo

Um atacante poderia navegar na URL http://vitima.com/index.php?page=admin/secretpage, que, se acessada, pode fazer com que a página de índice execute a secretpage.php, anteriormente protegida. Algumas vezes, ataques LFI permitem que um atacante acesse arquivos no sistema do servidor web fora do diretório raiz da *web*.

- bancos de dados e ataques de injeção SQL — muitos *sites* utilizam bancos de dados, um sistema que armazena informação de maneira organizada e produz relatórios sobre essa informação, com base em consultas apresentadas por usuários. Normalmente, invasores se interessam em acessar informações armazenadas em um banco de dados (Figura 8). Portanto, a maioria das interações com banco de dados baseadas em *web* é realizada fora do servidor, de maneira invisível para o usuário, de modo que as interações entre os usuários e o banco de dados possam ser cuidadosamente controladas. O objetivo de um atacante, obviamente, consiste em romper essa interação controlada com o banco de dados para obter acesso direto a ele.

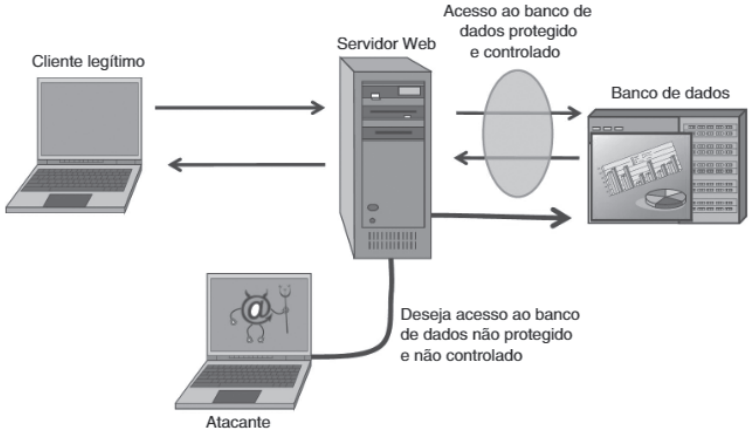

Figura 8. Interações de usuários com um servidor *web* que usa um banco de dados.
Fonte: Goodrich e Tamassia (2013).

Vulnerabilidades em protocolos para internet

Outra forma de classificação dos ataques é em relação aos protocolos TCP/IP. Segundo Forouzan e Fegan (2009), os protocolos para a internet, também conhecidos por protocolos TCP/IP, são distribuídos em cinco camadas: aplicativo, transporte, rede, enlace de dados e física. Na camada de aplicativos, temos protocolos como HTTP (*Hypertext Transfer Protocol*), FTP (File Transfer Protocol), DNS (*Domain Name System*), SMTP (S*imple Mail Transfer Protocol*), entre outros.

Já na camada de transporte, temos os protocolos TCP (*Transmission Control Protocol*, Protocolo de Controle da Transmissão), UDP (*User Datagram Protocol* - Procolo de ´ Datagrama do Usuário), SCTP (*Stream Control Transmission Protocol*).

Na camada de rede temos o protocolo IP (*Internetworking Protocol*), que suporta ICMP (*Internet Control Message Protocol*), IGMP (*Internet Group Management Protocol*), ARP (*Address Resolution Protocol*) e RARP (*Reverse Address Resolution Protocol*).

Por fim, nas camadas física e de enlace de dados, temos os protocolos que são definidos pelas redes subjacentes, como MAC (*Media Access Control Address*), NDP (*Neighbor Discovery Protocol*), entre outros.

Estes protocolos são vulneráveis às falhas como SYN *flooding* (ataca o TCP), IP *spoofing* (IP, e-mail e DNS), sequestro de sessão (HTTP), *source routing* e ataques ICMP (IP, ICMP), discutidos anteriormente. Mas, adicionalmente, segundo *Alotaibi et. al.* (2017) existem problemas de segurança que são mais recorrentes nas camadas de aplicativo, transporte e rede do TCP/IP, conforme descrito a seguir:

- Camada de aplicativo: no HTTP podem ocorrer ataques de *caching*, sequestro de sessão, ataques de repetição, e envenenamento de *cookies*. No protocolo DNS, os ataques mais frequentes são sequestro de ID DNS, DNS *spoofing* e envenenamento de cache DNS.
- Camada de transporte: técnicas para escaneamento de portas TCP/UDP, ataque TCP LAND (Local *Area Network Denial*), ataque de meia varredura de IP, ataque de geração de número de sequência TCP e SYN *flooding.*

- Camada de rede: tentativas de força bruta de senha, *spoofing,* HTTP *flooding, click jacking*, negação de serviço, detecção de pacotes, coleta ilegal de dados, sequestro e intercepção de conexões, restabelecimento da conexão, roteamento *multicast,* ataques *Smurf* e *Fraggle* (ataques distribuídos de negação de serviço).

Há também outros ataques, como o Source Routing, que é uma variação de IP *spoofing*, onde o *host* de origem pode especificar a rota que o receptor deve usar para responder. Adicionalmente, há os ataques de crackers, quando um *host* é violado para ser usado como meio para outros alvos, por meio da instalação de trojans ou outras ferramentas, e os ataques de *script kiddies*: por exemplo, quando um site é "pixado", ou os dados da página inicial são modificados por pessoas inexperientes, que usam códigos desenvolvidos por hackers profissionais.

Para a proteção ou defesa contra esses ataques cujo alvo são os protocolos para internet, é importante o uso de criptografia nos protocolos e o isolamento físico. Outras três técnicas que podem ser utilizadas para a proteção contra as vulnerabilidades são a filtragem de pacotes, uso de autenticação e *firewalls*. Segundo Forouzan e Fegan (2009), no nível IP, pode ser utilizado o IPSec (*IPSecurity*) é composto por uma coleção de protocolos que oferece segurança a um pacote IP. Já na camada de aplicativo, uma alternativa para a segurança no envio de e-mails é o PGP (*Pretty Good Privacy)*, que se utiliza de assinatura digital e criptografia. Concluindo, é importante ter conhecimento tanto das técnicas de ataque quanto dos possíveis mecanismos de defesa, para que possamos melhor gerenciar a segurança em equipamentos que façam parte de redes de computadores.

Referências

CANALTECH. *O que é DoS e DDoS?* 2018. Disponível em: <https://canaltech.com.br/produtos/O-que-e-DoS-e-DDoS/>. Acesso em: 17 dez. 2018.

FLEXDOCS. *Certificados digitais*. 2018. Disponível em: <http://www.flexdocs.com.br/guianfe/certificado.servidor.html>. Acesso em: 17 dez. 2018.

GOODRICH, M, T.; TAMASSIA, R. *Introdução à segurança de computadores*. Porto Alegre: Bookman, 2013.

OAB. *Visualizando os certificados instalados*. 2018. Disponível em: <http://cert.oab.org.br/m_ie_1c.html>. Acesso em: 17 dez. 2018.

PADILHA, R. *99 Conceitos Ilustrados de Hospedagem*: tentando compreender um vendedor de Startup. 18 jul. 2015. Disponível em: <http://midiasocialparanegocios.blogspot.com/2015/>. Acesso em: 17 dez. 2018.

TCP. *Uma conexão normal cliente-servidor*: o aperto de mão em três etapas é realizado corretamente. 22 jan. 2012. Disponível em: <https://pt.wikipedia.org/wiki/SYN_Flood#/media/File:Tcp_normal.svg>. Acesso em: 17 dez. 2018.

Leituras recomendadas

HD STORE. *Quais os tipos de ataques cibernéticos existentes?* 2018. Disponível em: <https://blog.hdstore.com.br/tipos-ataques-ciberneticos/>. Acesso em: 17 dez. 2018.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. *Hackers expostos*: segredo e soluções para a segurança de redes. 7. ed. Porto Alegre: Bookman, 2015.

NAKAMURA, T. E.; GEUS, P. L. *Segurança de Redes em ambientes coorporativos*. São Paulo: Novatec, 2007.

A legislação sobre a segurança da informação no mundo

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Explicar os aspectos comuns quanto à privacidade de dados nos mais diversos países.
- Reconhecer a importância do Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (GDPR–EU).
- Descrever as leis de proteção de dados em outros países americanos.

Introdução

O marco zero da relação entre instituições e indivíduo é a transparência, que possibilita maior liberdade na sociedade. Por vezes, o meio de garantir a transparência é a legislação. Quando está em jogo a segurança da informação, as leis de proteção de dados entram em cena. Por meio delas, é possível verificar e auditar se os dados transacionados estão sendo utilizados adequadamente, e não para outros fins que não aqueles previamente acordados.

Diversos países têm criado leis relativas à privacidade de dados. O RGPD, que em inglês tem a sigla GDPR (*General Data Protection Regulation*), por exemplo, é compartilhado pelos países da União Europeia (UE). Por meio do RGPD, esses países buscam padronizar e normatizar as suas legislações, bem como atingir conjuntamente os resultados esperados.

Neste capítulo, você vai estudar a legislação relativa à segurança da informação utilizada no mundo. Além de conhecer melhor o RGPD, você vai se familiarizar com a legislação de outros continentes. Como você vai notar, as prerrogativas legais se tornam cada vez mais universais. Afinal, no mundo todo, um simples dado pode proporcionar ganhos estratégicos para as organizações, porém sempre é necessário agir dentro da lei.

1 Proteção de dados internacional

O RGPD já está em vigor na UE desde 2018. No Brasil, a Lei Geral de Proteção de Dados (LGPD) já foi aprovada, porém ainda não está vigorando. Essas duas leis se unem a diversas legislações existentes no globo que também visam à proteção de dados dos cidadãos. Afinal, em um mercado cada vez mais digital e sem fronteiras, são necessárias algumas regulações para preservar as premissas básicas da individualidade das pessoas.

Cada país busca identificar as suas particularidades e características ao criar uma lei, porém é normal avaliar as iniciativas em andamento no resto do mundo para identificar o que deu certo e o que deu errado. Atualmente, o RGPD inspira os demais países, pois a não adequação às normas do mercado europeu se reflete no distrato comercial. Esse regulamento exige diversos cuidados, podendo inviabilizar acordos e até mesmo gerar multas aos envolvidos. Ou seja, os países que não se adequarem ao RGPD terão dificuldades para negociar com o bloco europeu.

A seguir, você vai ver como alguns países tratam a proteção de dados em seus territórios (GONZÁLEZ, 2020).

Alemanha

A Alemanha é um dos países pioneiros na regulamentação relativa à privacidade e à proteção de dados. A sua Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz* — BDSG), de 2017, segue os preceitos do RGPD. A BDSG trata dos direitos e deveres de órgãos públicos e privados para as atividades de coleta e processamento de dados. Além disso, há diretrizes específicas que determinam como as empresas devem e podem tratar os dados de seus funcionários.

Austrália

Na Austrália, a lei máxima sobre segurança e proteção de dados é a Lei de Privacidade, de 1988, que governa tanto as instituições do setor público quanto as do setor privado. A lei foi construída com base nos 13 Princípios Australianos de Privacidade (*Australian Privacy Principles* — APPs), que discorrem sobre temas como:

- uso e divulgação de dados;
- direitos do titular dos dados;
- manutenção da qualidade dos dados;
- transparência e anonimidade.

A lei é complementada pelas regulamentações estaduais de privacidade e pelas leis de proteção de dados voltadas para setores específicos.

China

A mais recente regulamentação chinesa sobre privacidade é a lei Tecnologia da Informação: Especificação Sobre Segurança de Informações Pessoais. Conhecida também apenas como "O Padrão", a regulamentação traz diretrizes sobre transparência, direitos do titular e consentimento. Antes de essa lei entrar em vigor, em 2017, o conjunto de regras chinesas sobre o tema era formado por diferentes regulamentações, como:

- Lei Civil da República Popular da China, de 2017;
- Lei de Cibersegurança, de 2017;
- Lei Criminal, de 2015;
- Decisão de Fortalecer a Proteção das Redes de Informações, de 2012;
- Padrão Nacional de Segurança da Tecnologia da Informação, de 2013;
- Lei de Proteção ao Consumidor, de 2014.

Dinamarca

Na Dinamarca, as principais regras sobre o tema estão na Lei Dinamarquesa de Proteção de Dados, de 2018. Anteriormente, a questão era regida pela Lei Dinamarquesa de Processamento de Dados Pessoais, estabelecida em 2000. A lei mais recente serve como complemento e reforço ao RGPD. Dessa forma, a lei dinamarquesa trata de processamento de dados, divulgação de informações pessoais, consentimento, transferência de dados, etc., além de estabelecer multas para casos de violação.

Filipinas

Em 2016, o país implementou a Lei nº 10.173, também conhecida como "Lei de Privacidade de Dados". Redigida quatro anos antes, em 2012, essa é a principal legislação sobre o tema nas Filipinas. A lei determina que, para que possa ser feita a coleta dos dados de um indivíduo, ele tem o direito de saber quem a realiza, com que propósito e com que finalidade. Ele também tem o direito de saber como e por quem os dados serão processados e quem terá acesso a eles.

Finlândia

A Finlândia substituiu sua Lei de Dados Pessoais, de 1999, pela Lei de Proteção de Dados, de 2018, visando a alcançar um maior alinhamento com o RGPD. Contudo, o país ainda tem outras regulamentações sobre proteção de dados específicas para setores do mercado e da indústria, como a Lei de Proteção da Privacidade dos Trabalhadores (Lei nº 759/2004) e o Código de Sociedade da Informação (Lei nº 917/2014), voltado para a confidencialidade de mensagens, *cookies* e telecomunicações.

França

A França é outro exemplo de país da UE que atualizou suas normas de proteção de dados para seguir mais explicitamente o RGPD. O país trocou sua Lei de Proteção de Dados pela Lei 2 de Proteção de Dados. A nova regulamentação estabelece as regras para os agentes de tratamento, determinando também que quaisquer tratamentos de dados devem ser feitos para fins específicos e que apenas os dados fundamentais para tais propósitos podem ser coletados. Além disso, a segunda versão da lei firma o direito do titular de saber quem é o agente de tratamento e qual é o propósito da coleta e do tratamento.

Grécia

A Grécia encontra-se em processo de elaboração de uma nova lei de proteção de dados, que já nascerá alinhada com o RGPD. Enquanto isso, a regulamentação vigente é a Lei nº 2.472/97, que traz regras para controladores e operadores e visa a garantir os princípios da transparência, do tratamento de dados com propósito e da responsabilização dos agentes. O país conta também com duas regulamentações adicionais sobre o tema: o Diretivo de Privacidade Eletrônica (Lei nº 3.471/2006), com normas complementares à lei principal, e o Diretivo de Retenção de Dados (Lei nº 3.917/2011), que trata do armazenamento de dados.

Índia

A Índia ainda não tem uma única lei central sobre proteção e privacidade de dados, e sim diversas leis e normativas que se complementam. Porém, o país publicou a Lei de Proteção de Dados Pessoais em dezembro de 2019, em análise por uma comissão parlamentar até a data da escrita deste capítulo. Enquanto

isso, as normativas mais importantes são a Lei de Tecnologia da Informação (Lei nº 21/2000) e a lista de Regras de Tecnologia da Informação, de 2011. Ambas trazem regras específicas sobre como proteger dados pessoais e outros requerimentos para garantir a privacidade de dados. Há, ainda, conjuntos de regras voltados especificamente para a coleta e o tratamento de dados pessoais nos setores bancário e de saúde.

Indonésia

O conjunto de regras sobre proteção de dados na Indonésia se constitui pela Lei de Informação e Transações Eletrônicas (Lei nº 11/2018) e sua respectiva emenda, pela Lei nº 19/2016 e pelas Regulações nº 82/2012 e nº 20/2016 (Regulação MOCI). Assim como a Índia, a Indonésia também vem trabalhando em uma lei que unifique suas regras sobre o tema: a Lei de Proteção à Privacidade de Dados Pessoais, baseada em grande parte no RGPD. O objetivo é que o texto da lei foque em consentimento, notificação de vazamentos de dados e exclusão de dados, entre outros pontos relacionados.

Islândia

Em 2018, a Islândia substituiu sua antiga Lei de Processamento de Dados Pessoais (Lei nº 77/2000) pela Lei de Proteção de Dados e Processamento de Dados Pessoais (Lei nº 90/2018) — também com o objetivo de adequar suas regras às do RGPD. A lei de 2018 traz diretrizes sobre como obter consentimento do titular, quando e como informar o titular sobre tratamentos realizados com seus dados, como armazenar dados devidamente e como fazer transferências internacionais de dados.

Japão

Desde 2003, a privacidade de dados era regida pela Lei de Proteção de Informações Pessoais (Lei nº 57/2003). Contudo, em 2017, o Japão colocou em prática a Emenda APPI, que traz preceitos básicos para a proteção de dados pessoais. A Emenda APPI traz regras sobre compartilhamento de dados com terceiros, manutenção de informações em bancos de dados e anonimização de dados e vazamentos, estabelecendo diretrizes para proteger os titulares. Devido à nova legislação, o Japão foi incluído na "lista branca" da UE, que reúne países com leis adequadas de proteção de dados.

Malásia

Em 2010, a Malásia colocou em vigor a sua primeira legislação sobre o tema, a Lei de Proteção de Dados Pessoais (Lei nº 709). Ela é construída sobre sete princípios: generalidade, notificação e escolha, divulgação, segurança, retenção, integridade de dados e acesso. Essa lei estabelece que, para que um tratamento de dados seja legítimo e legal, o titular deve receber informações por escrito sobre o propósito da coleta e do tratamento, sobre os seus direitos enquanto titular dos dados e sobre quem terá acesso a esses dados.

Nova Zelândia

A Nova Zelândia controla a privacidade de dados por meio dos 12 Princípios da Privacidade de Informação, estabelecidos em 1993 na Lei de Privacidade do país. Os princípios são focados principalmente em questões como propósito da coleta de dados, formas de armazenamento e acesso, limitações do tratamento e divulgação de dados pessoais. O país também tem legislações de privacidade voltadas para setores específicos, incluindo crédito, saúde e telecomunicações.

Saiba mais

Até a data da escrita deste capítulo, circulava pelo governo neozelandês a Lei de Privacidade de 2018 — que, quando aprovada, substituirá a legislação anterior. As mudanças mais significativas incluem reporte mandatório sobre vazamentos, notificações de *compliance* e fortalecimento de transferências internacionais de dados. Outra diretriz importante da nova legislação é o direito do titular de fazer uma reclamação sobre a legitimidade de uma coleta ou de um tratamento de dados, que subsequentemente será investigada.

Algumas considerações

Como você viu, a questão da privacidade de dados não é novidade. Afinal, diversos países já possuem legislações a respeito desse tema. O que fica cada vez mais claro é que o RGPD é a espinha dorsal das legislações que têm surgido. Ele indica o mínimo necessário para que haja cuidado com os dados individuais durante as transações comerciais (PINHEIRO, 2018).

A seguir, veja alguns aspectos comuns às diferentes leis nacionais (PINHEIRO, 2018):

- o cuidado que as empresas precisam ter com os dados dos cidadãos;
- a penalidade a que as empresas estão expostas caso haja algum tipo de vazamento;
- a noção de que o usuário é o dono dos seus dados, de modo que precisa saber o pode ser feito com o dado que disponibiliza durante determinada transação.

Na Figura 1, veja o grau de aderência dos países às leis de proteção de dados. Como você pode notar, a Argentina e o Uruguai são os países sul-americanos mais aderentes às leis de proteção de dados. Destaca-se também a Guiana Francesa, país que está sujeito às leis francesas e, por consequência, adere totalmente à legislação europeia (SERPRO, 2020).

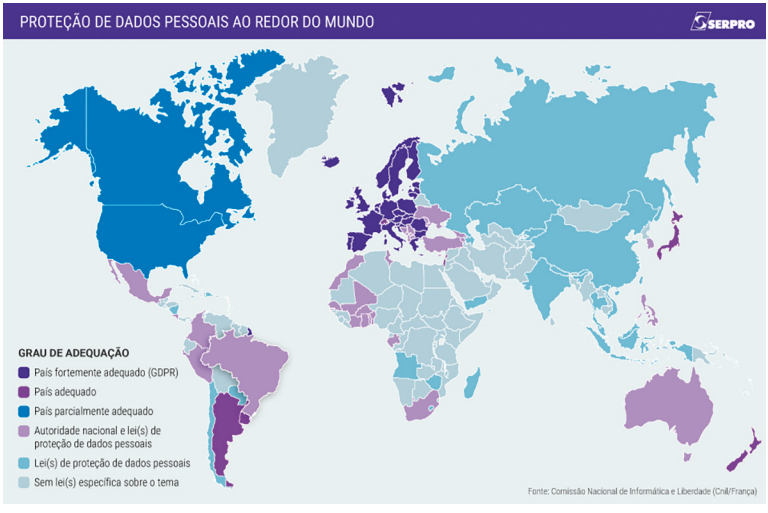

Figura 1. Adequação dos países à proteção de dados.

Fonte: Serpro (2020, documento *on-line*).

2 RGPD

No dia 27 de abril de 2016, foi consolidado o RGPD. Ele discorre sobre a proteção das pessoas físicas no que diz respeito ao correto tratamento dos dados pessoais e à utilização desses dados pelos mercados, o que implica considerar o livre fluxo de dados (*free data flow*).

Ficou acordado que a lei entraria efetivamente em vigor após dois anos, quando seriam colocadas em prática as penalidades pertinentes. Até então, as penalidades não seriam aplicadas, pois o momento seria de transição e adequação de todas as partes interessadas. Conforme Pinheiro (2018), a implementação do RGPD gerou um efeito dominó, tendo em vista que todos os países que não pertencem à UE enfrentariam algumas barreiras e até mesmo sofreriam impactos financeiros caso não aderissem à legislação da zona do euro. Em um mundo cada vez mais competitivo, os países tiveram de se adaptar às novas exigências para fazer negócios com esse mercado tão importante.

O objetivo do RGPD (UNIÃO EUROPEIA, 2016) é contribuir para a obtenção de um espaço de liberdade, segurança e justiça. Além disso, o RGPD visa à união econômica para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e o bem-estar das pessoas físicas. Esse regulamento ainda tem o intuito de assegurar um nível coerente de proteção das pessoas físicas no âmbito da UE e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno. A ideia é garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo.

Fique atento

São impostas obrigações e responsabilidades iguais aos controladores e processadores. O RGPD busca assegurar um controle coerente do tratamento dos dados pessoais, possibilitando a cooperação efetiva entre as autoridades de controle dos diferentes Estados-membros.

Vale a pena destacar que, apesar de essa lei reforçar a importância fundamental das informações dos cidadãos, ela acaba apenas complementando diversas outras leis nacionais existentes no bloco europeu, como a Carta dos Direitos Fundamentais da UE e o Tratado sobre o Funcionamento da UE. Nesse sentido, é possível fazer um paralelo com o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) e a Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011), ambos do Brasil (PINHEIRO, 2018).

No entanto, essa regulamentação se faz necessária no sentido de esclarecer conceitos ambíguos e não factíveis. Foi nesse ponto que o RGPD inovou em relação às demais leis, buscando também padronizar as normas relativas aos atributos qualitativos cobrados e penalizados.

No Quadro 1, a seguir, veja como o RGPD põe em prática os itens de conformidade relativos à proteção de dados. Note que esse regulamento busca esclarecer a necessidade do cuidado com os dados e exemplificar os procedimentos adequados, indicando como os dados devem ser tratados, protegidos e disponibilizados.

Quadro 1. Itens de conformidade em relação ao regime europeu

Item de conformidade	Regime europeu (RGPD)
Definição e distinção do que são dados pessoais e dados sensíveis. Tal conceituação busca delimitar os direitos e as informações protegidas pelo ordenamento jurídico.	Define que dado pessoal é qualquer informação que identifique ou torne identificável a pessoa natural. Já dados sensíveis são dados pessoais sobre etnia, raça, crenças religiosas, opiniões políticas, dados genéticos/biométricos, além de informações sobre filiações a organizações quaisquer. O RGPD também faz considerações acerca dos dados genéticos, biométricos e relativos à saúde.
Obrigatoriedade do consentimento do usuário para a coleta de informações e limitação do tratamento do dado conforme finalidade.	Prevê a necessidade de uso do dado conforme a finalidade apontada. Traz exceções de tratamento por motivo de interesse público, segurança e saúde.

(Continua)

(Continuação)

Quadro 1. Itens de conformidade em relação ao regime europeu

Item de conformidade	Regime europeu (RGPD)
Distinção entre titularidade e responsabilidade sobre os dados, assim como delimitação das funções e responsabilidades assumidas no tratamento de dados.	Titular é a pessoa natural a quem se referem os dados que são objeto de tratamento; por outro lado, o responsável é a pessoa física ou jurídica, de direito público ou privado, que realiza decisões sobre o tratamento de dados. O controlador é quem realiza as decisões acerca do tratamento de dados; o processador, quem efetua o tratamento dos dados. Ambos são responsáveis pelo tratamento dos dados.
Indicação de um encarregado pela comunicação entre os agentes, titulares e órgãos competentes.	Aponta que o controlador deve ter uma pessoa responsável por tudo que seja relacionado à proteção de dados (DPO).
Aplicação de mecanismos e práticas pautadas no livre acesso à informação e na transparência entre os usuários e as organizações.	Os titulares têm direito a informações claras e acessíveis do início ao fim do tratamento do dado, podendo revogar o consentimento a qualquer momento.
Aplicação de medidas de segurança e dever de reportar.	As empresas devem criar medidas — como pseudonimização e encriptação de dados — para garantir a segurança de forma preventiva. No caso de qualquer incidente, a notificação às autoridades deve ser imediata.
Possibilidade de alteração e exclusão do dado pessoal.	Os titulares dos dados podem alterar ou excluir seus dados.
Aplicação de sanções no caso de descumprimento das regras.	Prevê a aplicação de sanções gradativas e multas administrativas, que podem chegar a 20 milhões de euros ou a 4% do faturamento anual da empresa.
Criação de um órgão competente para fiscalizar e zelar pela proteção de dados pessoais e pela privacidade.	Possui um órgão de controle e fiscalização de proteção de dados pessoais por Estado (28) e aplica o princípio do balcão único.

Fonte: Adaptado de Pinheiro (2018).

3 Leis de proteção de dados nas Américas

Nas Américas, conforme Lemos *et al*. (2018), a legislação de proteção dos dados vem ganhando maturidade e mais protagonismo. Isso ocorre tanto devido a escândalos de vazamento de dados (como no caso do Banco Inter, que na época perdeu seu certificado digital) quanto pelo uso de informações para eleições (como no caso da Cambridge Analytica e do Facebook nas eleições dos Estados Unidos em 2016). A seguir, você vai ver como alguns países da América tratam a proteção de dados em seus territórios (GONZÁLEZ, 2020).

Argentina

A Lei de Proteção de Dados da Argentina (Lei nº 25.326) estabelece que a coleta de dados só pode ser feita mediante o consentimento do usuário. A lei, que se aplica a qualquer pessoa ou entidade que lida com dados pessoais no país, diz ainda que o titular dos dados (o indivíduo a quem as informações se referem) tem o direito de acessar, corrigir, deletar e solicitar a exclusão de seus dados. Porém, para deixar as regras de proteção de dados do país mais alinhadas às tendências mundiais estabelecidas pelo RGPD, a Argentina vem trabalhando em uma nova lei sobre o tema, que terá a legislação atual como base e irá ainda mais além — determinando, por exemplo, uma abordagem mais completa e obrigações mais rígidas.

Brasil

No Brasil, há a LGPD — que foi aprovada, porém, até a data de escrita deste capítulo, ainda não estava em vigor, mas já vem promovendo mudanças significativas na forma como as empresas coletam e tratam dados. O direito à privacidade já havia sido estabelecido pelo art. 5 da Constituição Federal de 1988 e pelo Código de Proteção ao Consumidor, instituído em 1990. Outra importante legislação sobre o tema no País é o Marco Civil da Internet, sancionado em 2014. Voltado inteiramente para o uso da internet no País, o Marco Civil traz princípios, garantias, direitos e deveres dos usuários da rede, além de diretrizes sobre como o Estado deve atuar. Ao lado da privacidade, alguns dos outros principais temas abordados são:

- neutralidade da rede;
- retenção de dados e funções sociais da internet, como liberdade de expressão;
- transmissão de conhecimento e responsabilidade civil.

Canadá

O país conta com um total de 28 regulamentações — entre leis provinciais e federais — que tratam das questões de privacidade e proteção de dados. A legislação nacional referente a isso é a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (*Personal Information Protection and Electronic Documents Act* — Pipeda). Válida para todas as províncias do Canadá, a Pipeda apresenta diretrizes referentes à coleta, ao tratamento e à divulgação de dados pessoais coletados por empresas durante o exercício de suas atividades comerciais. Além disso, discorre sobre as transferências internacionais e inter-regionais de dados pessoais. Como complemento a ela, há legislações similares aplicáveis em Alberta, Colúmbia Britânica e Quebec. Estabelecida em 2000, a Pipeda opera com base em 10 princípios de boas práticas a serem seguidos pelas empresas (bastante similares às bases da LGPD brasileira). São elas:

1. as empresas são responsáveis pelos dados pessoais que coletaram e que usam;
2. é preciso identificar claramente os propósitos por trás de uma coleta de dados;
3. é preciso ter o consentimento do titular para coleta, uso e compartilhamento de seus dados, salvo exceções previstas por lei;
4. podem ser coletados somente os dados necessários dentro do propósito informado;
5. os dados solicitados podem ser usados, divulgados e mantidos pela empresa apenas da maneira informada e enquanto cumprirem os propósitos;
6. as informações pessoais devem ser verídicas e mantidas atualizadas;
7. os dados devem ser protegidos por medidas adequadas, de acordo com a sensibilidade das informações;
8. a organização precisa fornecer amplamente informações claras e detalhadas sobre suas políticas e práticas de segurança e proteção de dados;
9. o titular dos dados tem o direito de receber informações sobre a existência de tratamentos de suas informações, assim como de questionar se seus dados são verídicos e estão completos;
10. o titular dos dados tem o direito de questionar as organizações que tratam e coletam suas informações pessoais, dentro dos nove princípios anteriores.

Colômbia

Na Colômbia, a questão da privacidade e da proteção de dados é regida por quatro regulamentações: o Decreto nº 1.377/2013, a Lei nº 1.581/2012, a Lei nº 1.273/2009 e a Lei nº 1.266/2008. O Decreto nº 1.377/2013 aborda o consentimento do titular, as transferências internacionais de dados e as políticas de processamento de dados pessoais. Enquanto isso, a Lei nº 1.581/2012 estabelece o direito de cada indivíduo de determinar como seus dados serão coletados, armazenados, usados, processados e transferidos — além de regulamentar os direitos à privacidade na coleta e no processamento de dados pessoais. A Lei nº 1.273/2009, por sua vez, traz diretrizes sobre crimes cibernéticos e estabelece que roubar, vender ou comprar dados pessoais é uma atividade criminosa. Finalmente, a Lei nº 1.266/2008 discorre sobre a privacidade de dados no que tange a dados comerciais e financeiros.

Estados Unidos

Os Estados Unidos não têm apenas uma lei que governe a privacidade de dados, e sim diversas legislações específicas para diferentes setores ou vigentes em determinados estados. Há cerca de 20 leis voltadas para um único setor ou indústria em âmbito nacional, além de outras cem legislações estaduais de privacidade — o estado da Califórnia é o "lar" de 25 delas. A principal lei californiana de privacidade é a Lei de Privacidade do Consumidor da Califórnia (*California Consumer Privacy Act* — CCPA), que garante aos consumidores quatro direitos básicos sobre seus dados pessoais: de serem notificados, de terem acesso, de poderem optar (ou não) por uma coleta de dados e de terem acesso igualitário a serviços.

Todas as empresas que coletam e/ou tratam dados de cidadãos californianos precisam seguir a CCPA, e não apenas aquelas com sede no estado. Nacionalmente falando, as mais importantes regulamentações são a Lei de Privacidade, de 1974, a Lei de Proteção à Privacidade, de 1980, a Lei Gramm–Leach–Bliley, de 1999, a Lei de Portabilidade e Responsabilidade dos Seguros de Saúde, de 1999, e a Lei de Relatório de Crédito Justo, de 2018. Além disso, os Estados Unidos têm alguns acordos especiais de proteção à privacidade com a UE e a Suíça.

México

A questão da privacidade de dados no México é regida pela Lei Federal de Proteção de Dados Pessoais em Poder de Particulares — ou seja, estão em jogo dados coletados e tratados por empresas privadas. A lei foi estabelecida em 2010. Essas organizações também são governadas pelas diretrizes da lista de Regulamentações da Lei Federal de Proteção de Dados Pessoais em Poder de Particulares, instituída em 2011, pelas Orientações de Notificações de Privacidade, de 2013, e pelos Parâmetros de Autorregulamentação, de 2014. Para gerenciar todas essas regras, garantir a devida implementação e administrar penalidades, o México conta com o Instituto Federal de Acesso à Informação e Proteção de Dados (Ifai).

Algumas considerações

Da mesma forma que os demais países, conforme Pinheiro (2018), aqueles localizados no continente americano têm reforçado o cuidado com os dados dos cidadãos. Além disso, têm buscado aplicar a devida penalidade quando as empresas expõem informações de maneira indevida. Ademais, nos países americanos, também é consenso que os usuários têm o direito de saber o que será feito com as suas informações.

Como você viu ao longo deste capítulo, a proteção dos dados pessoais é essencial em um ambiente comercial cada vez mais complexo e dinâmico, em que as fronteiras entre o certo e o errado precisam ser claras para viabilizar uma sociedade melhor.

Referências

GONZÁLEZ, M. *Conheça o cenário das leis de proteção de dados ao redor do mundo*. 2020. Disponível em: https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/. Acesso em: 13 abr. 2020.

LEMOS, R. *et al. GDPR*: a nova legislação de proteção de dados pessoais da Europa. 2018. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018. Acesso em: 16 abr. 2020.

PINHEIRO, P. P. *Proteção de dados pessoais*: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2018.

SERPRO. *Em que "estágio" estamos?* Confira o mapa da proteção de dados pessoais no mundo. 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais. Acesso em: 13 abr. 2020.

UNIÃO EUROPEIA. *Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.* Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). 2016. Disponível em: https://eur-lex. europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.POR&toc=OJ:L: 2016:119:FULL. Acesso em: 13 abr. 2020.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

editora
papervest

Publicação da Papervest Editora
Av. Marechal Floriano, 947 - CEP: 88503-190
Fone: (49) 3225-4114 - Lages / SC
www.unifacvest.edu.br