NÃO PODE FALTAR

SEGURANÇA DE REDES

Emilio Tissato Nakamura

CONTROLE DE SEGURANÇA

O controle de segurança mais famoso é o *firewall*, que é o responsável pelo controle de acesso de rede.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

PRATICAR PARA APRENDER

Nesta seção, você reforçará e aprofundará o entendimento dos princípios da segurança da informação (confidencialidade, integridade e disponibilidade), dos elementos do risco (ativos, vulnerabilidades,

agentes de ameaça, ameaças, probabilidade e impacto) e dos relacionamentos com mecanismos de defesa, controles de segurança e técnicas de segurança de redes.

Para os profissionais de segurança da informação que buscam prevenção, detecção e resposta, é preciso entender onde, por que e como os ataques acontecem. Nesta seção, vamos detalhar alguns desses ataques e conhecer alguns controles de segurança que podem ser utilizados para a prevenção e detecção.

Para você alcançar a melhor estratégia de segurança, é importante entender que os elementos que compõem o risco de segurança se inter-relacionam o tempo todo. Por exemplo, ataques de negação de serviço (*Denial of Service*, DoS) afetam a disponibilidade e podem ser realizados por crackers que exploram vulnerabilidades em protocolos de rede. Há, ainda, outras variáveis que devem ser entendidas sobre os ataques DoS e tudo o que está envolvido, desde os pontos de ataques até os controles de segurança que podem ser aplicados.

Lembre-se de que os controles de segurança atuam sobre as vulnerabilidades que existem em ativos, e os agentes de ameaça exploram essas vulnerabilidades existentes em ativos. Quando isso acontece, uma ameaça se torna um incidente de segurança, o que causa impactos para a empresa.

Você é o responsável pela segurança da informação de uma empresa do setor químico que conta com os maiores cientistas brasileiros e possui unidades em São Paulo, Rio de Janeiro e Salvador. Além disso, ela tem acordo de cooperação internacional com uma empresa chinesa e outra suíça, bem como tem parceria com grandes investidores para o financiamento de seus projetos.

A sua atividade será focada em um grande projeto em andamento que já chegou a grandes resultados, uma vez que os cientistas descobriram um novo composto que será utilizado na indústria agrícola. Você, no

entanto, está preocupado com a forma como os resultados do desenvolvimento estão sendo protegidos. O impacto pode ser gigantesco em caso de incidentes de segurança, principalmente com a concorrência também mobilizando grandes equipes para colocar no mercado os avanços para o setor.

Nesta disciplina, você já sensibilizou a diretoria executiva da empresa quanto à necessidade de ações para a segurança do projeto. Você fez uma apresentação envolvendo, conceitualmente, elementos do risco, como ativos, agentes de ameaça, vulnerabilidades, ameaças, impactos e controles de segurança, fazendo uma conexão com os princípios da segurança da informação (confidencialidade, integridade e disponibilidade).

Nesta segunda rodada de apresentação para a diretoria executiva, você detalhará os seguintes elementos:

- Pontos de ataques, representados por sistemas compostos por diferentes aspectos, que possuem vulnerabilidades: *hardware*, *software*, protocolos, aplicações.
- Pontos de ataques indicando os ativos humanos e físicos envolvidos.
- Agentes de ameaça, ameaças e técnicas de ataques.
- Controles de segurança para a autenticação dos usuários.
- Controles de segurança de rede.

Considere que o projeto está em execução pelas pessoas que têm as ideias e que essas informações vão, de forma digital, do *notebook* até o servidor da empresa, passando pela rede, e que nesse caminho as informações podem ser vazadas, alteradas ou destruídas (CID).

Você pode **fazer um diagrama ou relacionar todos os elementos em uma lista**, bem como fazer um **breve resumo** de cada caso ou situação presente nela. Por exemplo: uma situação que os diretores executivos precisam saber é que um *cracker* (agente de ameaça) pode explorar uma vulnerabilidade do sistema operacional do servidor (ativo) para

contaminar o sistema com um *exploit* (técnica de ataque) e roubar (ameaça) as informações do novo composto químico (ativo). Apresente as situações envolvendo DoS, DDoS, ataque de força bruta e ataque do homem do meio.

No final da apresentação, **apresente uma sugestão de conjunto de controles de segurança**, indicando quais situações cada um deles mitiga. A diretoria executiva, então, saberá que há diversos pontos de ataques e diferentes situações de segurança que podem ser resolvidos com a sua proposta de estratégia de segurança contendo um conjunto de controles.

Vamos, agora, explorar o mundo dos ataques que viraram notícias no mundo da segurança e que tanto afetam as empresas. É o entendimento dos assuntos desta seção que fará você compreender melhor o mercado de trabalho de segurança da informação, que sofre transformações constantes em linha com as evoluções dos ataques cibernéticos, dos novos negócios, das novas tecnologias e das novas ameaças.

CONCEITO-CHAVE

INCIDENTES DE SEGURANÇA

Em agosto de 2020, a bolsa de valores da Nova Zelândia sofreu paralisação de suas operações em virtude de ataques de negação de serviços por quatro dias (CPOM, 2020). Ataques de *ransomware*, que sequestram dados de servidores e usuários com a finalidade de resgates, continuam fazendo vítimas em todo o mundo (CRN, 2020).

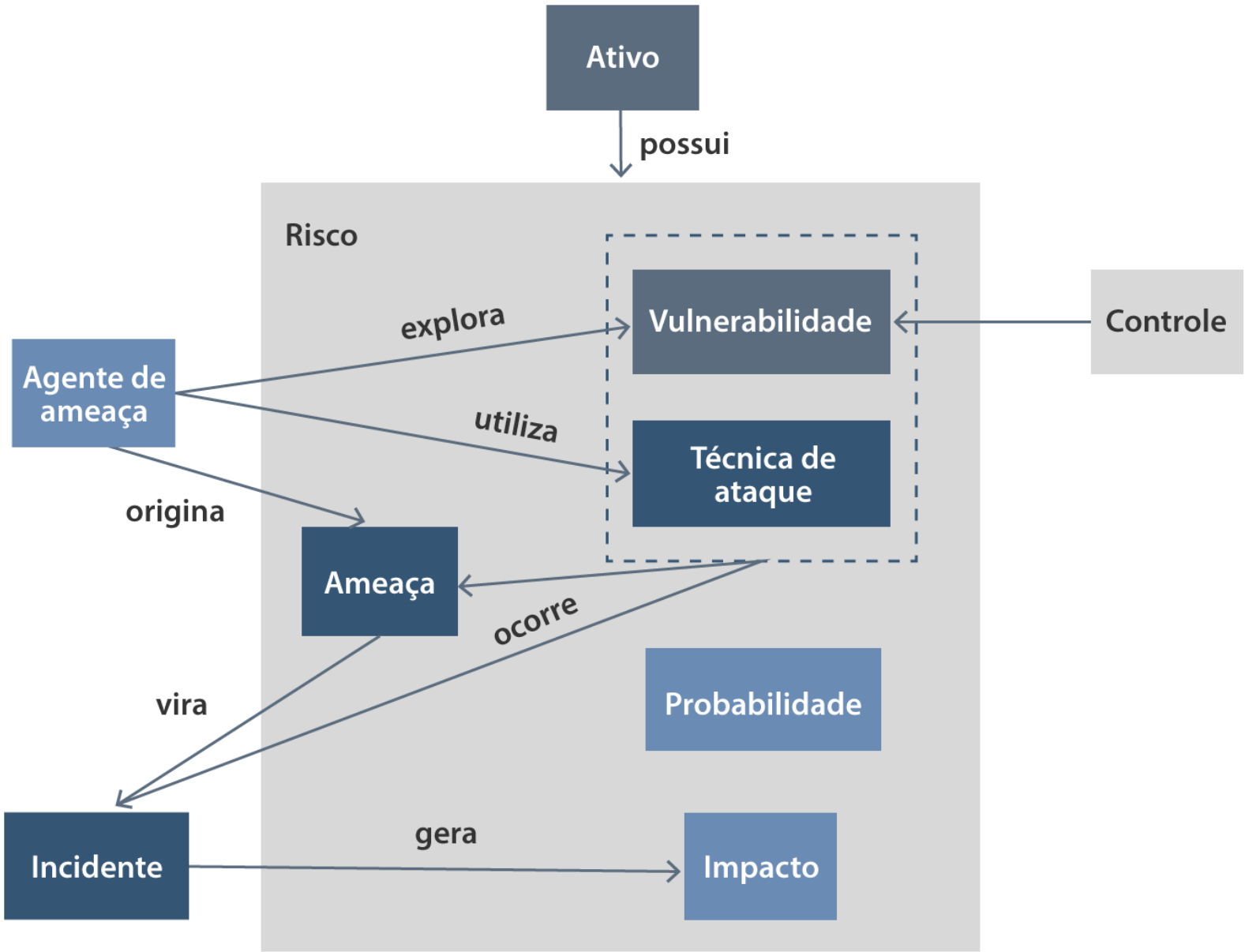
Esses dois casos mostram que os ataques de crackers ou ataques cibernéticos continuam acontecendo e evoluindo numa alta velocidade, atingindo desde pequenos negócios até infraestruturas críticas de países.

O que há de comum entre os dois ataques citados é que eles podem ter sido causados pelos mesmos agentes de ameaça, os *crackers*, e resultaram em grandes impactos para as suas vítimas. Há, no entanto, um conjunto de elementos diferentes, que vai desde a ameaça até a técnica de ataque utilizada, a vulnerabilidade explorada, o princípio da segurança da informação atingido e o ponto de ataque ou ativo

explorado, e são esses elementos que serão discutidos nesta seção, de modo que você possa entender a complexidade e as possibilidades de ataques existentes.

A Figura 1.2 mostra os elementos do risco. Agentes de ameaça exploram, com técnicas de ataques, as vulnerabilidades de ativos, e, quando isso ocorre, uma ameaça se torna um incidente de segurança. Como profissional de segurança, você deve conhecer esses elementos e, a partir do cálculo do risco (probabilidade e impacto), estabelecer uma estratégia de segurança com os controles de segurança a serem implementados.

Figura 1.2 | Fluxo com componentes de risco de segurança da informação

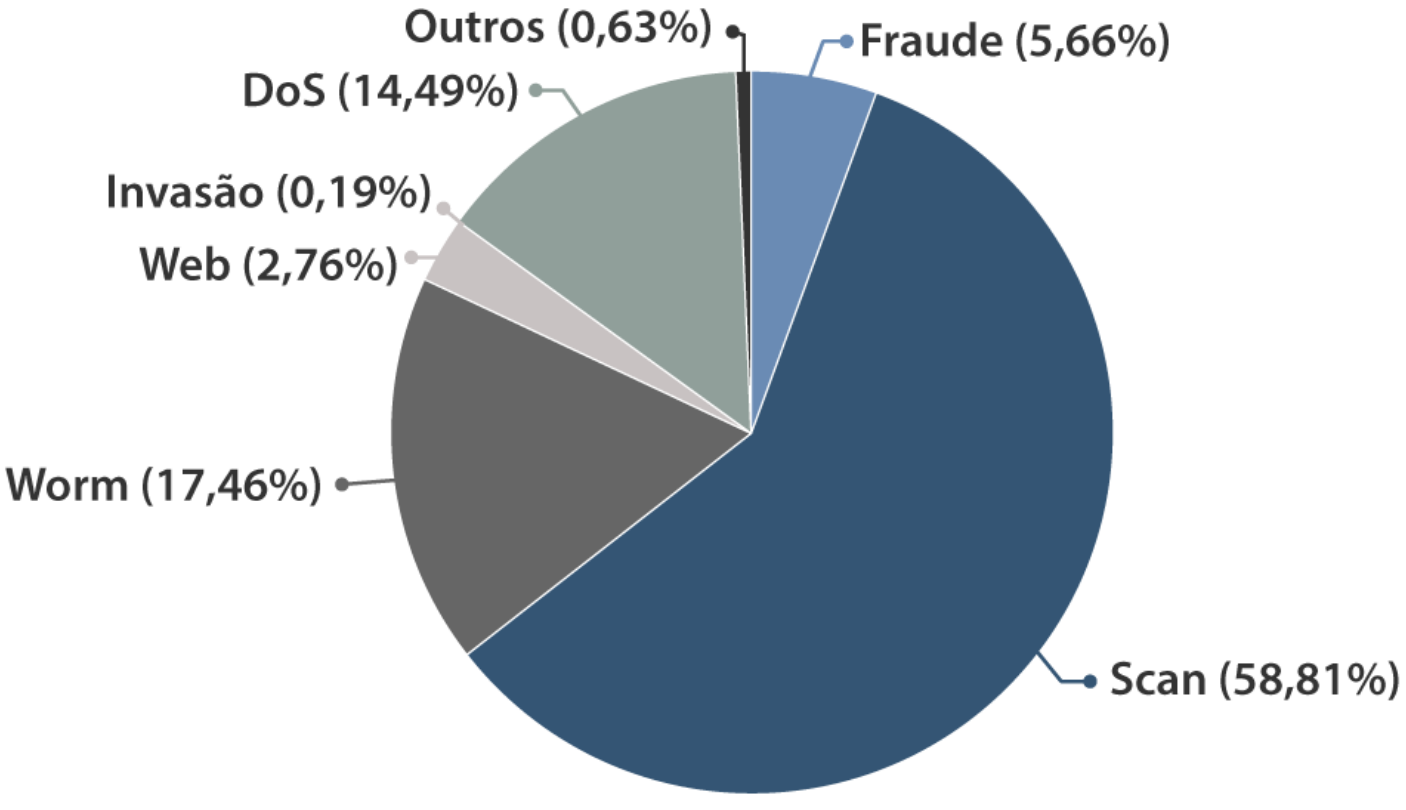


Fonte: elaborada pelo autor.

O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. Ele é responsável por tratar incidentes de segurança em computadores que envolvem redes conectadas à Internet no Brasil. A Figura 1.5 apresenta os incidentes de segurança reportados ao CERT.br de janeiro a junho de 2020, enquanto o Quadro 1.1 apresenta os ataques que fazem parte da estatística (CERT, 2020).

Figura 1.5 | Incidentes de segurança reportados ao CERT.br (janeiro a junho de 2020)

Tipos de ataque



Ver anotações 0

Fonte: adaptada de: CERT.br.

Quadro 1.1 | Definição para os incidentes de segurança reportados ao CERT.br

worm	Notificações de atividades maliciosas relacionadas ao processo automatizado de propagação de códigos maliciosos na rede.
DoS	Notificações de ataques de negação de serviço, em que o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, um computador ou uma rede.
invasão	Um ataque bem sucedido que resulta no acesso não autorizado a um computador ou rede.
Web	Um caso particular de ataque visando especificamente ao comprometimento de servidores Web ou desfigurações de páginas na Internet.
scan	Notificações de varreduras em redes de computadores com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
fraude	Segundo Houaiss (2001, p. 1388), é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Essa categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de se obter vantagem.
outros	Notificações de incidentes que não se enquadram nas categorias anteriores.

Fonte: adaptado de CERT.br (2007).

A partir desse entendimento da dinâmica dos ataques, você pode definir a melhor estratégia de segurança da informação, composta pelos elementos do risco para justificar as definições, e os controles de segurança a serem implementados.

VOCABULÁRIO

Hackers ou *crackers*? Segundo Nakamura e Geus (2007), os *hackers*, por sua definição original, são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos à vítima, mas sim como um desafio às suas habilidades. Eles invadem os sistemas, capturam ou modificam arquivos para provar a sua capacidade e compartilham a sua proeza com seus colegas, demonstrando que conhecimento é poder. Exímios programadores e conhecedores dos segredos que envolvem as redes e os computadores geralmente não gostam de ser confundidos com *crackers*. Com o advento da Internet, os diversos ataques pelo mundo foram atribuídos a *hackers*, mas eles refutam essa ideia, dizendo que hacker não é *cracker*. *Crackers* são elementos que invadem sistemas para roubar informações e causar danos à vítima. *Crackers* também é uma denominação utilizada para aqueles que quebram códigos e proteções de *softwares*. Com o crescimento da Internet e a consequente facilidade em se obter informações e ferramentas de ataques, a definição de *hacker* mudou. A própria imprensa mundial tratou de mudar esse conceito. Muitas vezes, um incidente de segurança é atribuído a *hackers*, em seu sentido genérico (NAKAMURA; GEUS, 2007).

OS PONTOS DE ATAQUES

Ativos são atacados pelos agentes de ameaça, que exploram as suas fraquezas ou pontos fracos ou vulnerabilidades. Em segurança da informação, a definição da estratégia de segurança é desafiadora justamente porque um *cracker* pode concretizar o seu ataque explorando uma única vulnerabilidade de um único componente ou ativo de um sistema. Por outro lado, você, como profissional de segurança, deve ser capaz de enxergar todas essas possibilidades, definir e implementar os controles de segurança que protegem a sua empresa. Isso deve ser feito de acordo com uma visão de riscos, ou seja, você deve definir os controles de acordo com as prioridades que resultam da avaliação da probabilidade e do impacto envolvido com cada ameaça existente.

E os pontos de ataques são muitos em um sistema (LIMA, 2017). Imagine que sua empresa disponibiliza um portal de fornecedores; nesse cenário, quais são os pontos de ataques que devem ser considerados?

> **REFLITA**
>
> A segurança da informação visa garantir os princípios da confidencialidade, integridade e disponibilidade da informação.
>
> A informação possui diferentes dimensões:
>
> - Ela pode estar na cabeça das pessoas.
> - Ela pode estar em um meio físico, como em um pedaço de papel ou cunhado na parede de uma caverna.
> - Ela pode estar em um meio digital, como em um *smartphone*, em um servidor, na nuvem ou sendo transmitido pelo ar, por meio de ondas de rádio, por exemplo.

> Isso faz com que tenhamos que pensar em controles de segurança que vão além dos aspectos tecnológicos, tais como a conscientização de usuários e o controle de acesso físico. Os controles de segurança devem, assim, ser utilizados em conjunto, formando uma defesa em camadas.

No caso do portal de fornecedores, há um conjunto de elementos ou ativos que fazem parte do sistema e que podem, assim, conter vulnerabilidades que são visadas pelos agentes de ameaça. Há, no portal de fornecedores, além da aplicação, o banco de dados, o *middleware*, o sistema operacional, o servidor, a comunicação ou a rede e os administradores que possuem o acesso a esses componentes. Todos eles representam pontos de ataques que podem levar à perda de confidencialidade, integridade ou disponibilidade.

Há, nesse exemplo, potenciais vulnerabilidades de *hardware* (servidor, disco rígido), *software* (aplicação, *middleware*, banco de dados, sistema operacional), protocolos (TCP/IP ou outro utilizado pela aplicação). Como tudo passa pela rede e a aplicação está na camada 7 da pilha de protocolos TCP/IP, o portal de fornecedores está sujeito às vulnerabilidades de rede e de *hardware*.

Além disso, não podemos deixar de lado as vulnerabilidades humanas, relacionadas aos administradores de sistemas, e as vulnerabilidades físicas, relacionadas ao *datacenter*.

Os pontos de ataques também devem ser avaliados de acordo com o estado da informação. A informação pode estar em processamento, também conhecido como Data-In-Use (DIU), ou em transmissão, conhecido como *Data-In-Motion* (DIM). Quando a informação está armazenada, o estado é conhecido como *Data-At-Rest* (DAR).

EXEMPLIFICANDO

Ver anotações

Com a **Lei Geral de Proteção de Dados Pessoais** (LGPD), os dados pessoais devem ser protegidos para a garantia da privacidade. Ataques podem ser realizados para que dados pessoais sejam vazados e a privacidade seja comprometida, bem como podem ocorrer com dados em processamento (DIU), dados em transmissão (DIM) ou dados armazenados (DAR). Ataques a banco de dados visam aos dados armazenados, enquanto ataques à rede visam aos dados em transmissão. Já os dados em processamento podem sofrer ataques mais sofisticados.

AGENTES DE AMEAÇA, AMEAÇAS E TÉCNICAS DE ATAQUES

Os agentes de ameaça são elementos importantes para o entendimento dos riscos e da segurança; os mais comuns são as pessoas, que possuem facetas diferentes, de acordo com o ambiente em avaliação. Por exemplo, os ***crackers***, a depender do contexto, são pessoas maliciosas que atacam sistemas de informação, mas há outras pessoas que também podem comprometer a sua empresa. Será que um funcionário mal-intencionado também não pode atacar a sua empresa? **Fraudadores** também são pessoas que podem atacar a sua empresa, explorando vulnerabilidades de funcionários desatentos, por exemplo. E há, ainda, os **agentes de ameaça naturais**, que podem comprometer a disponibilidade da informação em caso de uma inundação de datacenter, por exemplo.

Um agente de ameaça bastante crítico, que pode ser considerado também uma ameaça, é o ***malware*** ou o código malicioso. *Malwares* são programas desenvolvidos com o objetivo de gerar alguma ação danosa ou maliciosa em um computador. Existem diversos tipos de *malware* e cada um age de uma maneira; vírus e *worm* são exemplos.

VOCÊ SABE A DIFERENÇA ENTRE UM VÍRUS E UM WORM?

Vírus é um código malicioso que contamina um sistema a partir de uma ação do usuário. Por exemplo: um clique em um link contaminado, que contém um vírus que explora uma vulnerabilidade do sistema, ou a instalação de um *software* suspeito, tornando-se parte de outros programas e arquivos. Já aquele código malicioso que se propaga automaticamente nas redes em busca de uma vulnerabilidade do sistema operacional, por exemplo, contaminando e se espalhando sem a necessidade de ação humana, é chamado de ***worm***.

Outro exemplo de *malware* é o **cavalo de Troia**, que o usuário instala em seu sistema imaginando que o *software* executa somente aquela função que ele buscava, mas que, na realidade, realiza ações maliciosas, como o *keylogger*, para capturar o que o usuário digita ou a gravação e o envio de arquivos para o *cracker*.

> **EXEMPLIFICANDO**
>
> Um ataque bastante comum que visa ao roubo de credenciais de acesso a bancos é o uso de *keylogger*. Quando o equipamento do usuário é contaminado com esse *malware*, tudo o que é digitado, como a senha bancária, é enviado ao *cracker*.

Outro tipo de *malware* é o ***Backdoor***. Esse código malicioso possibilita que o invasor realize acessos remotos não autorizados ao sistema sem que, muitas vezes, seja percebido. O *Backdoor* explora vulnerabilidades no sistema, por exemplo, *softwares* ou *firewall* desatualizados, pela abertura de portas, por exemplo, servidor, do roteador e *firewall*.

Há ainda, casos em que *backdoors* são inseridos por fabricantes de programas de forma proposital, com a justificativa de administração do sistema (CERT.BR, 2020).

> **PESQUISE MAIS**
>
> Para entender melhor os *malwares*, tais como os vírus, *worm*, *bot* e *botnet*, *spyware*, *backdoor*, cavalo de Troia (*trojan*) e *rootkit*, acesse a Cartilha de Segurança do CERT.BR.
>
> - CERT.br. **Cartilha de Segurança para internet.** [s.d.].

Um *malware* crítico é o ***ransomware***; ele sequestra informações com o uso de criptografia. O criminoso cifra os arquivos ou o disco e exige o pagamento de um resgate em troca da chave criptográfica que decifra as informações originais.

> **REFLITA**
>
> Em meados de 2017, um *ransomware* chamado *WannaCry* trouxe sérios transtornos para muitas instituições, inclusive no Brasil. O cibercriminoso bloqueia o acesso a recursos por meio de criptografia e a vítima só consegue descriptografá-los após o pagamento de um resgate. Qual princípio da segurança da informação você considera que foi violado: confidencialidade ou integridade dos dados? O que pode ser feito para evitar ou minimizar os impactos desse tipo de ataque?

Agora, vamos discutir outro tipo de **ataque que afeta a disponibilidade da informação**. A informação pode existir em diferentes estados (DIM, DIU, DAR), e entender o fluxo dela do servidor para o usuário é importante para identificar como a disponibilidade pode ser afetada.

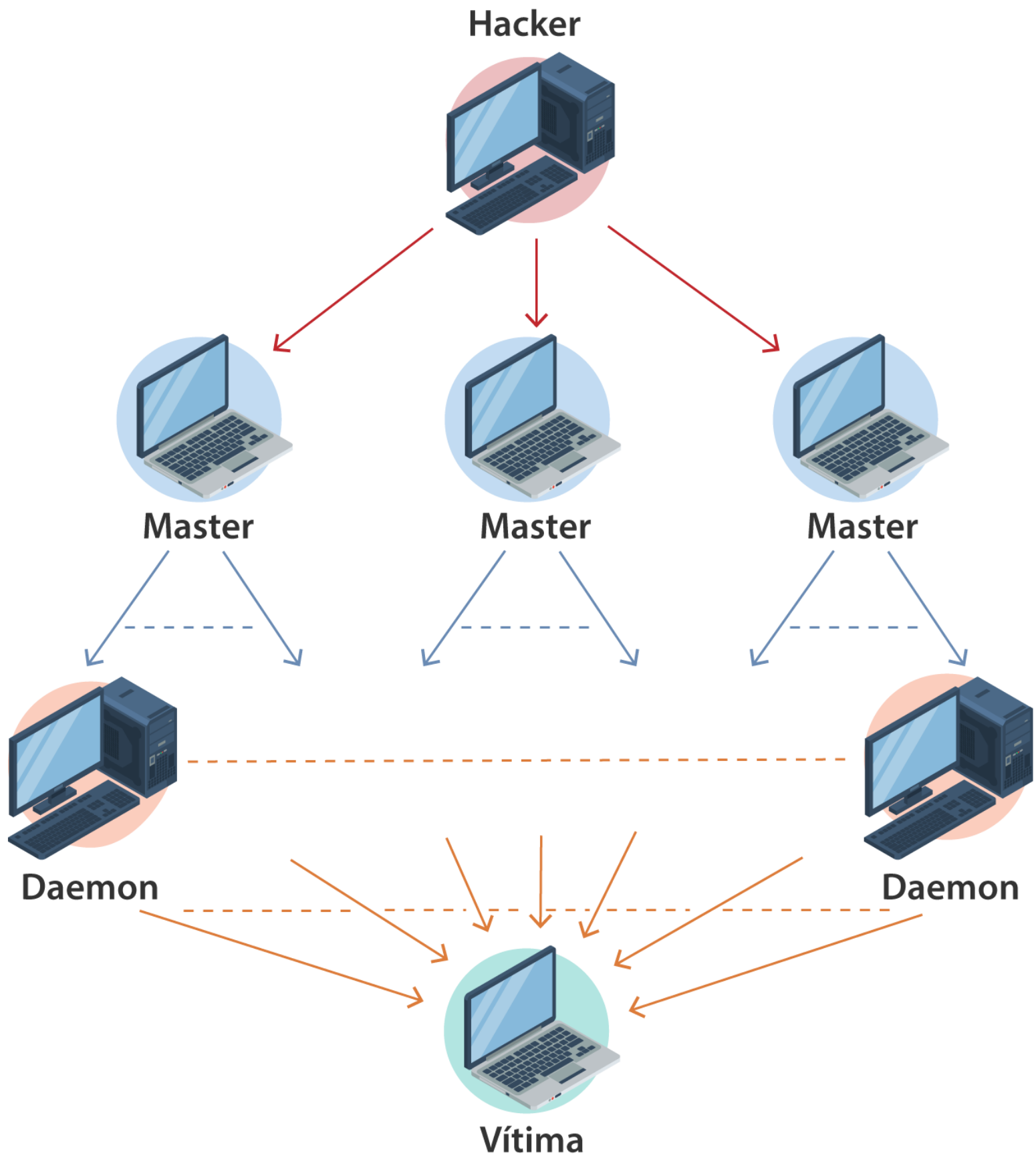
De forma geral, uma informação que está em um banco de dados (DAR) pode ser acessada por um usuário, e o fluxo passa pela aplicação, que pode fazer um processamento (DIU) antes de ser enviado pela rede (DIM), mas não sem antes passar pelo sistema operacional, e esses são os pontos em que a informação pode ser atacada.

No caso da disponibilidade, o ataque mais tradicional é a **negação de serviço ou *Denial-of-Service* (DoS)**, que pode ser direcionado para qualquer um desses pontos de ataque. Imagine uma quantidade tão grande de requisições que uma aplicação não é mais capaz de atender. Não precisa nem mesmo ser um ataque, já que, em muitas ocasiões, o acesso a determinado serviço pode se tornar impossível quando há muitos acessos simultâneos, como para a compra online de ingressos ou o envio de documentos obrigatórios no final do prazo por todos os brasileiros. Quando há uma coordenação para que as requisições sejam enviadas simultaneamente, a partir de diferentes pontos, o ataque é conhecido como ***Distributed Denial-of-Service* (DDoS)**.

> **SAIBA MAIS**
>
> Há uma série de ataques de negação de serviço (DoS ou DDoS) que valem a pena ser conhecidos. Há o SYN *Flooding*, fragmentação de pacotes IP, *Smurf* e *Fraggle* e DDoS com distribuição e coordenação com o uso de *master*, *zombies* e *daemons*.

A Figura 1.6 apresenta um ataque DDoS, em que o atacante utiliza *masters* e *daemons* para o ataque distribuído e coordenado à vítima. Os *masters* são máquinas controladas diretamente pelo atacante, enquanto os *daemons* são controlados pelos *masters*. Os *daemons* realizam efetivamente o ataque à vítima.

Figura 1.6 | Ataque de DDoS



Fonte: elaborada pelo autor.

Os ataques DoS e DDoS podem tirar proveito também do próprio protocolo TCP com a manipulação das mensagens de conexão envolvendo o SYN (OLIVEIRA, 2017).

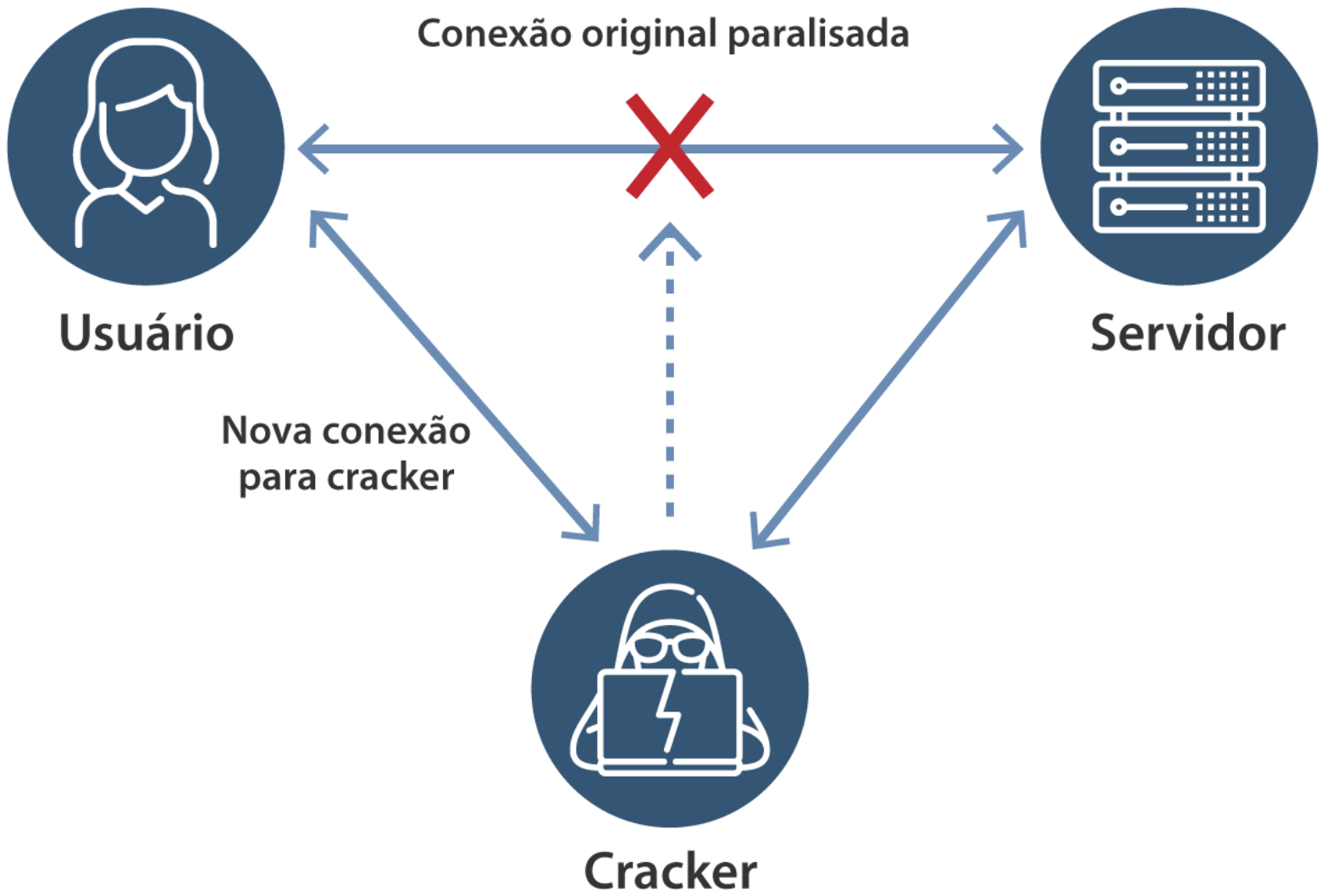
EXEMPLIFICANDO

Uma técnica típica de DoS é o SYN *Flooding*, que causa o *overflow* da pilha de memória por meio do envio de grande número de pedidos de conexão TCP, que não podem ser totalmente completados e manipulados. Essa técnica foi uma das utilizadas por Kevin Mitnick em um dos ataques mais

> conhecidos da internet (LUONG, 2007). Além desse ataque, outros ataques DoS e DDoS continuam acontecendo, comprometendo bancos, especialistas em segurança, provedores de serviços e de nuvem, entre outros (JUNQUEIRA, 2020).

Outro ataque importante é **o ataque do homem do meio ou *Man-In-The-Middle* (MITM)**, que pode ser visto na Figura 1.7.

Figura 1.7 | Ataque do homem do meio com redirecionamento de tráfego



Fonte: elaborada pelo autor.

Esse ataque é conhecido também como sequestro de conexões e é ativo, ou seja, a manipulação ocorre em tempo real, com o agente de ameaça tendo o controle dela, redirecionando as conexões TCP para determinada máquina.

Além da injeção de tráfego, permite, ainda, driblar proteções geradas por protocolos de autenticação, comprometendo, assim, a confidencialidade (tendo acesso às informações em trânsito), a integridade (alterando ou injetando informações na conexão) e mesmo a disponibilidade (descartando informações que deixam de chegar ao seu destino) (NAKAMURA; GEUS, 2007). Malenkivich (2013) cita alguns exemplos de ataques do homem do meio ou MITM.

Outro problema relacionado à autenticação dos usuários é que uma senha pode ser adivinhada (*password guessing*) ou descoberta com o uso de técnicas como o **ataque do dicionário**, em que palavras de dicionários são testadas, ou o **ataque de força bruta**, em que diferentes combinações de caracteres são testadas em busca do acesso.

Ver anotações

Assim, um dos mecanismos de segurança que podem ser utilizados é a trava de tentativas de acessos após determinado número de tentativas inválidas de senhas.

> **ASSIMILE**
>
> DoS e DDoS comprometem a disponibilidade da informação com a exploração de diferentes componentes de um sistema, como a rede ou a aplicação; já ataques envolvendo *malware* ou o ataque do homem do meio podem comprometer, além da disponibilidade, a confidencialidade e a integridade da informação.

CONTROLES DE SEGURANÇA E PROTEÇÃO

Já vimos os principais pontos de ataques e as relações entre agentes de ameaça, ameaças e as principais técnicas de ataques utilizadas. Agora, vamos complementar o entendimento com os controles de segurança e proteção, começando com a proteção à rede. Após uma discussão sobre *firewall*, *Intrusion Prevention System* (IPS) e *antimalware*, apresentaremos algumas das principais ferramentas de proteção de informações.

A proteção à rede considera que, no fluxo da informação, todo acesso passa pela rede, sendo este, portanto, um bom local para controles de segurança. De fato, uma boa estratégia de segurança deve levar em consideração a rede, com uma **arquitetura de redes segura, considerando segmentação, uso de zonas desmilitarizadas** (*DeMilitarized Zone*, DMZ), **controle de acesso de rede e detecção de ataques** (OLIVEIRA, 2017).

> **ASSIMILE**
>
> Em uma rede segura, a criação de uma zona desmilitarizada ou *DeMilitarized Zone* (DMZ) é uma técnica importante. Uma DMZ é uma rede específica que fica entre uma rede pública, como a Internet, e a rede interna. Com essa segmentação, a

rede interna conta com uma camada adicional de proteção, pois os acessos são permitidos para os serviços disponibilizados na DMZ, mas não para a rede interna.

O controle de segurança mais famoso é o ***firewall***, que é o responsável pelo controle de acesso de rede. Na realidade, o *firewall* começou funcionando na camada de rede e, atualmente, ele atua também na camada de aplicação, realizando a proteção contra ataques que vão além de ataques de rede, com o ***Web Application Firewall*** (WAF).

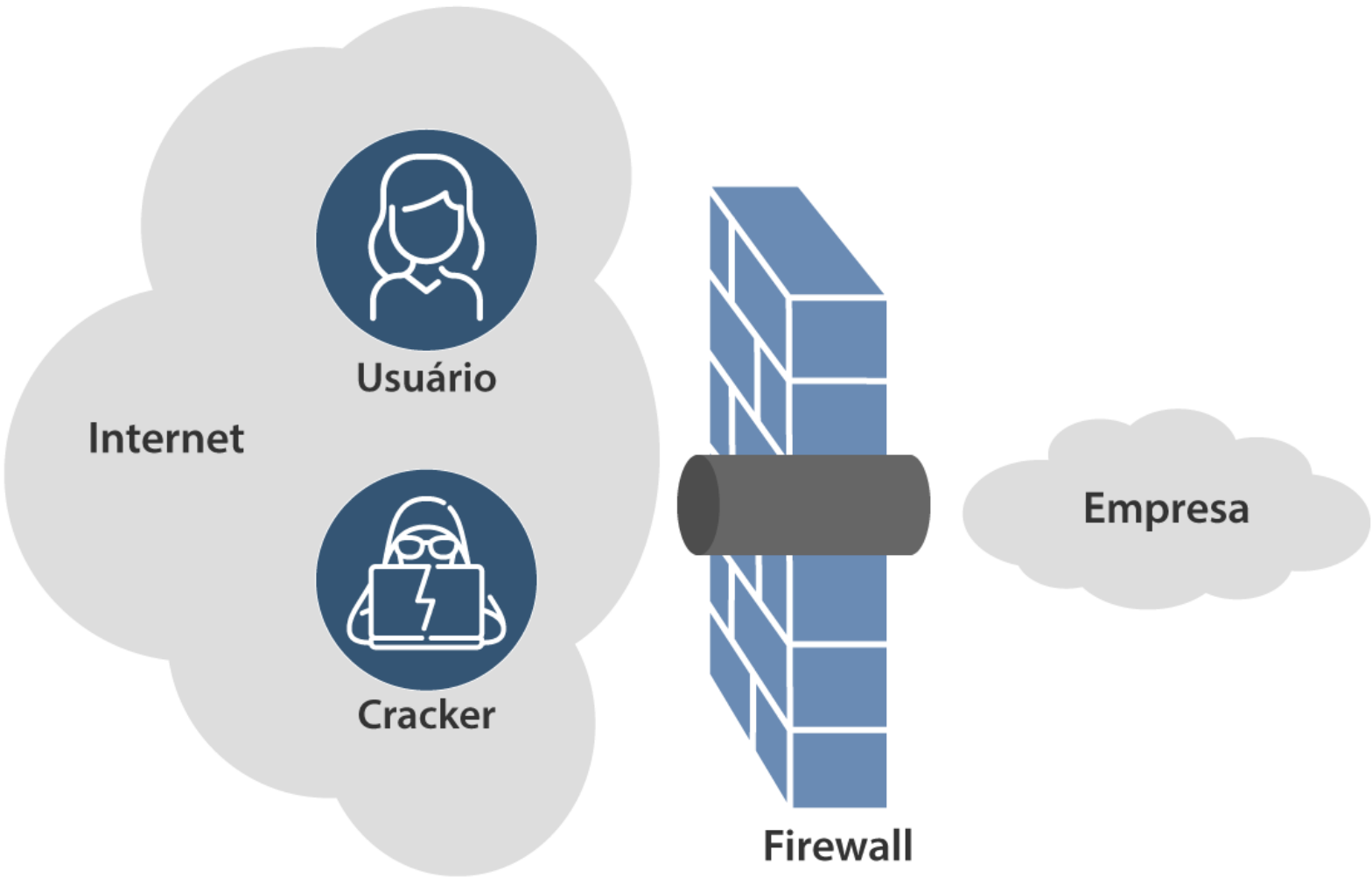
ASSIMILE

Um controle de segurança importante para proteger as aplicações é o *firewall* de aplicação web ou *Web Application Firewall* (WAF). Enquanto um *firewall* faz a filtragem do tráfego de rede baseado nos cabeçalhos dos pacotes, o WAF faz o filtro e monitora o tráfego entre os usuários e a aplicação Web na camada de aplicação HTTP.

Um *firewall* tradicional funciona como um avaliador de pacotes de rede, filtrando as conexões de acordo com os cabeçalhos dos pacotes e as regras definidas. Dessa forma, um dos principais desafios do uso do *firewall* é a sua configuração, composta por regras que consideram, pelo menos, os diferentes segmentos de rede, os serviços disponibilizados pela empresa e os serviços que podem ser acessados pelos usuários internos. A complexidade dessas regras pode fazer com que conexões que não devem passar pelo *firewall* consigam o acesso a recursos.

Na Figura 1.8, o *firewall* é configurado com regras que possibilitam algumas conexões para a empresa e que são utilizadas pelos usuários, mas que também podem ser utilizadas por um cracker para os ataques.

Figura 1.8 | *Firewall* possibilita algumas conexões com as regras



Fonte: elaborada pelo autor.

EXEMPLIFICANDO

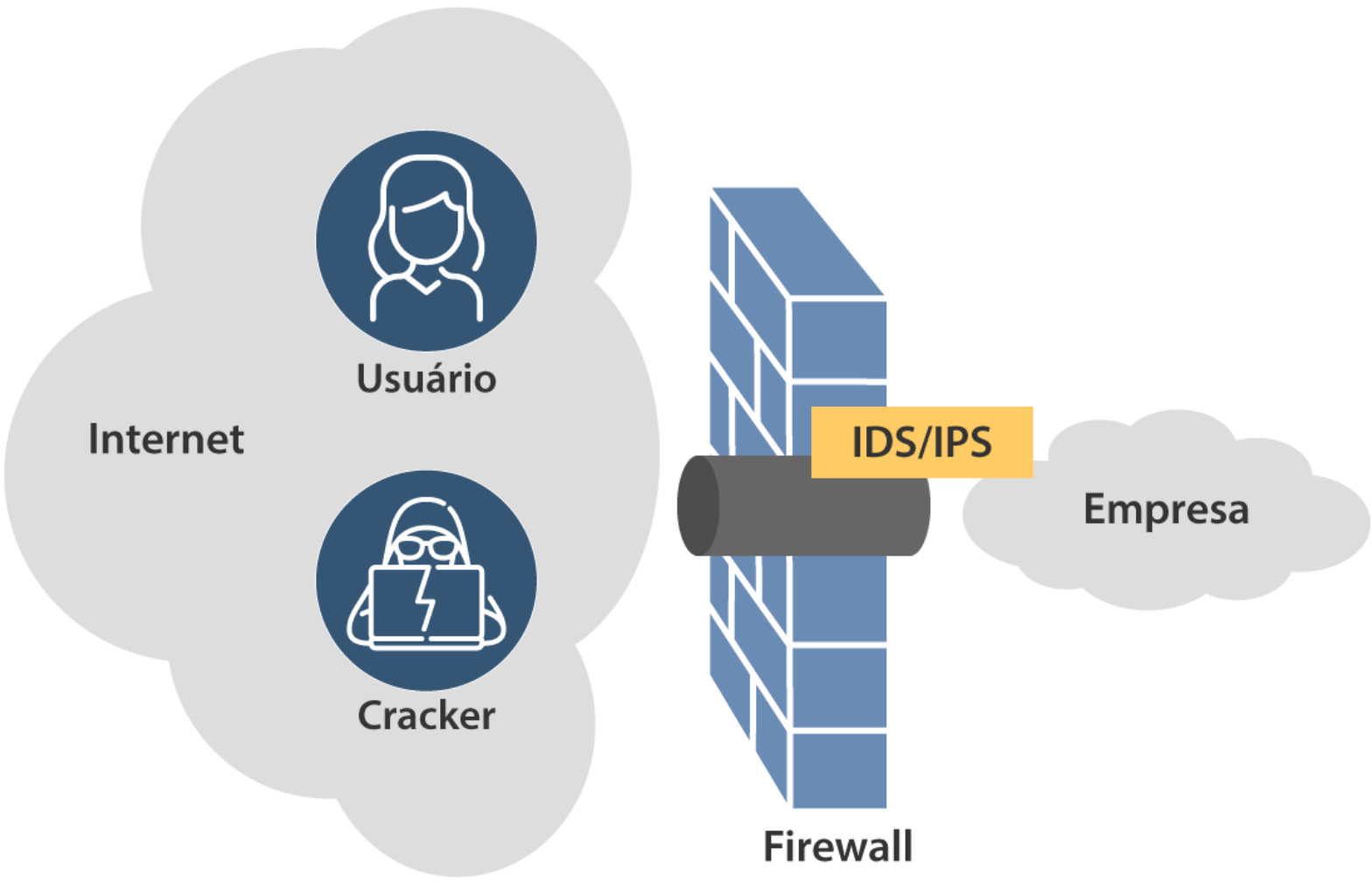
Um exemplo de aplicação é o *Microsoft Terminal Services*, cujo ***Remote Desktop Protocol*** **(RDP)** é um serviço disponibilizado pelo *Windows* para acesso remoto. O acesso remoto possibilita que acessos externos sejam feitos a equipamentos que, muitas vezes, estão na rede interna da empresa. Isso facilita atividades como administração remota ou suporte remoto, porém abre uma brecha significativa, que pode ser explorada em ataques. O *firewall* tem que liberar a porta TCP 3389 para que o RDP funcione, e, já que o *firewall* possibilita essas conexões, os ataques passam diretamente pelo *firewall*.

O *scan* de portas é uma técnica que possibilita a identificação de computadores ativos e a coleta de informações sobre os programas instalados e serviços existentes na empresa ou em determinada faixa de endereços IP. O *scan* de portas permite a descoberta de serviços como o RDP.

Assim, é importante que você saiba que a existência de um *firewall* na empresa é uma das principais fontes da falsa sensação de segurança, já que o papel dele é filtrar tudo aquilo que não é permitido. É como se um muro protegesse a sua empresa, mas uma série de portas ou furos existisse nesse muro para permitir as conexões necessárias para a sua empresa. Com isso, ataques aos serviços não podem ser protegidos por um *firewall* tradicional, já que as conexões, inclusive dos ataques direcionados àquele serviço, passam livremente pelo controle, uma vez que as regras permitem.

Reforçando a importância da defesa em camadas, o controle complementar ideal para o *firewall* é o sistema de detecção de intrusão ou ***Intrusion Detection System* (IDS)**. Esse controle de segurança analisa diferentes informações, como as conexões, os logs e os fluxos de dados para detectar ataques em andamento, em tempo real (Figura 1.9).

Figura 1.9 | IDS / IPS monitorando as conexões que passam pelo *firewall*



Fonte: elaborada pelo autor.

O ***Intrusion Prevention System*** **(IPS)** é uma evolução do IDS, funcionando não somente com a detecção de ataques, mas também tomando ações automáticas de contenção dos ataques em tempo real. Há vários aspectos a serem considerados na tecnologia, como a possibilidade de ataques que visam justamente à paralisação dos acessos aos serviços da empresa com o envio de mensagens que ativam o IPS, que, acreditando haver um ataque em andamento, fecha as conexões e impossibilita o acesso legítimo.

Os avanços tecnológicos continuam e os sistemas de detecção e prevenção de intrusão atuais incorporam técnicas de inteligência artificial para diminuir a quantidade de falsos positivos (alarmes falsos) e falsos negativos (ataques não detectados).

Um ponto importante a considerar é que o contexto da segurança da informação continua a sua evolução com o uso de nuvem (LIMA, 2017) e os perímetros das empresas alterando-se rapidamente, de modo que o ambiente corporativo atual vai além do perímetro físico da empresa e alcança os parceiros de negócios e a residência dos funcionários. Aliados à transformação digital, aspectos de segurança ganham ainda mais importância; com isso, os controles de segurança são essenciais também nos próprios dispositivos, constituindo, assim, a segurança de ponta ou segurança de *endpoint*. Os próprios *firewall*, IPS e *antimalware* fazem parte do arsenal de defesa dos *endpoints* ou dispositivos, complementando a segurança de redes.

Antimalware busca códigos maliciosos e, basicamente, funciona com a verificação de assinaturas ou códigos que identificam um *malware* já identificado anteriormente e que possui vacina específica. Se, por um lado, os códigos maliciosos podem alterar seu próprio código ou gerar polimorfismo para não serem detectados pelo *antimalware*, do outro lado, o controle de segurança adota, cada vez mais, a inteligência artificial para detectar comportamentos anômalos que podem representar perigo para as empresas.

Dessa forma, os controles de segurança de rede atuam não somente nos pontos de ataque de rede, mas também nos dispositivos dos usu��rios.

Outro conjunto de controles de segurança visa ao controle de acesso, tanto de usuários quanto de conteúdo. A **autenticação** é um dos principais controles de segurança ao validar a identidade dos usuários, a fim de que possam ter acesso aos recursos. Já vimos que o ataque de força bruta busca a descoberta da senha, que representa um fator de autenticação baseado em alguma coisa que o usuário sabe. Como há outros ataques, como a adivinhação de senhas ou o furto com o uso de *malwares* ou engenharia social, é importante considerar o uso de outros fatores de autenticação. Há possibilidade de usar códigos ou *Tokens* em dispositivos móveis, como os enviados via SMS (alguma coisa que o usuário possui) ou mesmo a biometria (alguma coisa que o usuário é). Quando dois fatores diferentes de autenticação, como a senha e o SMS, são utilizados, a autenticação é de duplo fator ou de múltiplo fator.

> **REFLITA**
>
> Em segurança, é preciso considerar aspectos de usabilidade e o nível de segurança requeridos para cada caso. No caso da autenticação, há três fatores utilizados tradicionalmente para a validação da identidade: algo que o usuário sabe, algo que o usuário possui e algo que o usuário é. Cada método de autenticação possui suas características tecnológicas que se somam aos aspectos de segurança e usabilidade. Por exemplo: o uso de SMS exige que o usuário esteja com a posse do dispositivo móvel no momento do acesso, mas a mensagem nem sempre chega para ele. Já as senhas precisam ser memorizadas, e a repetição de senhas não é recomendada, visto o número de incidentes de segurança envolvendo o vazamento de senhas de acesso de variados serviços, que acabam comprometendo outros. No caso da

> biometria, acessos públicos por meio da impressão digital, por exemplo, possuem reflexos na privacidade e em questões de higiene. Assim, cada tipo de acesso deve levar em consideração o nível de risco e os tipos de ataques existentes, bem como os aspectos de segurança e usabilidade envolvidos.

Ver anotações 0

Para finalizar, o **controle de conteúdo** faz parte dos controles de segurança das empresas ao filtrar o acesso a conteúdos impróprios ou que levam à perda de produtividade de seus funcionários. Normalmente, atuando em conjunto com o *firewall*, o filtro de conteúdo pode ser baseado em endereços web ou em palavras-chave.

Chegamos, assim, ao final desta seção, em que você pôde se aprofundar em aspectos fundamentais para a concepção da melhor estratégia de segurança para a sua empresa. Você viu que diferentes pontos de ataque podem ser explorados pelos agentes de ameaça: da aplicação ao sistema operacional, passando pelo *datacenter*, pela rede e pelos próprios funcionários, entre outros. Você viu, ainda, que há uma série de técnicas de ataques que pode ser utilizada pelos agentes de ameaça e que essas técnicas são variadas, passando de ataques de rede até ataques de aplicação, existindo, ainda, ataques aos próprios controles de segurança, como os ataques que comprometem a autenticação dos usuários. Tudo isso é importante para que você defina os controles de segurança mais condizentes com a sua empresa.

FAÇA VALER A PENA

Questão 1

Você é o analista de segurança de uma grande empresa do setor de energia. Durante uma avaliação de segurança periódica, você avalia os riscos, incluindo as vulnerabilidades. Considere um servidor de arquivos no *datacenter* com documentos confidenciais sobre salários de todos os empregados da empresa.

Os controles de segurança devem ser implementados

a. Somente no servidor de arquivos, porque não pode haver vulnerabilidades no *datacenter*.

b. Somente no *datacenter*, porque não pode haver vulnerabilidades no servidor de arquivos.

c. No servidor de arquivos e no *datacenter*, porque todas as vulnerabilidades devem ser eliminadas.

d. Somente no servidor de arquivos, porque não pode haver ataques ao *datacenter*.

e. Somente no *datacenter*, porque não pode haver ataques ao servidor de arquivos.

Ver anotações 0

Questão 2

Um *cracker* pode utilizar uma série de técnicas de ataques em diferentes pontos. Uma dessas técnicas é o DoS, que visa “derrubar” um servidor, impedindo os acessos legítimos, o que compromete a disponibilidade daquela informação.

Assinale a alternativa que corresponde ao caso de ataque de DoS referente ao exposto.

a. *Cracker* utilizou o DoS para roubar informações do servidor.

b. *Cracker* invadiu um banco de dados utilizando o DoS.

c. *Cracker* explorou um ataque de força bruta para “derrubar” o servidor.

d. *Cracker* explorou grande número de conexões para paralisar o servidor.

e. *Cracker* acessou uma informação invadindo um ponto de ataque do servidor.

Questão 3

Um *malware* bastante crítico é o *ransomware*, em que o criminoso cifra os arquivos ou o disco e exige o pagamento de um resgate em troca da chave criptográfica que decifra as informações originais.

Assinale a alternativa que apresenta o princípio da segurança da informação comprometido pelo *ransomware* e um possível controle de segurança para se lidar com o *malware*.

a. Disponibilidade e *firewall*.

b. Integridade e *firewall*.

c. Confidencialidade e *firewall*.

d. Confidencialidade e *backup*.

e. Disponibilidade e *backup*.

Ver anotações 0

REFERÊNCIAS

CERT.BR. **Cartilha de Segurança para Internet.** [s.d.]. Disponível em: https://cartilha.cert.br/malware/. Acesso em: 1 dez. 2020.

CERT.BR. **Incidentes reportados ao CERT.br -- janeiro a junho de 2020.** 2020. Disponível em: https://bit.ly/39KCd2a. Acesso em: 1 dez. 2020.

HOPE, A. **New Zealand stock exchange shut down by DDoS cyber attack.** 2020. Disponível em: https://bit.ly/2YIFRDk. Acesso em: 1 dez. 2020.

HOUAISS, A. **Grande dicionário Houaiss da Língua Portuguesa.** 1 ed. Rio de Janeiro: Ed. Objetiva, 2001.

LIMA, A. C. de. **Segurança na computação em nuvem.** São Paulo: Editora Senac, 2017.

MALENKOVICH, S. **O que é um Ataque Man-in-the-Middle?** 2013. Disponível em: https://bit.ly/2MUb5Vi. Acesso em: 1 dez. 2020.

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

NOVINSON, J. **The 11 Biggest Ransomware Attacks Of 2020 (So Far).** 2020. Disponível em: https://bit.ly/3at60vA. Acesso em: 1 dez. 2020.

OLHAR DIGITAL. **Confira 5 dos maiores ataques DDoS dos últimos anos.** 2020. Disponível em: https://bit.ly/3jfjiiZ. Acesso em: 1 dez. 2020.

OLIVEIRA, R. C. Q. **Segurança em redes de computadores.** São Paulo: Editora Senac, 2017.

SOUZA, R. de. **Relatório aponta aumento no número de ataques DDoS no segundo trimestre de 2020.** 2020. Disponível em: https://bit.ly/3rjlb0Y. Acesso em: 1 dez. 2020.

THE HACK. **The hack.** 2020. Disponível em: https://thehack.com.br. Acesso em: 1 dez. 2020.