NÃO PODE FALTAR

SEGURANÇA NA INTERNET

Emilio Tissato Nakamura

O QUE SÃO TRANSAÇÕES WEB?

Uma transação web pode ser uma compra online, uma transação bancária, a realização de algum serviço governamental ou até mesmo uma postagem em uma rede social, a qual envolve diferentes tipos de dados ou informações, dados pessoais, financeiros e confidenciais.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

CONVITE AO ESTUDO

Olá, nesta unidade, abordaremos tópicos do nosso cotidiano, em que há o uso cada vez mais intenso da internet para as atividades que vão desde a comunicação pessoal e profissional, passando por transações financeiras, compras virtuais e acesso a conteúdos especializados, chegando até ao cumprimento de obrigações como cidadãos brasileiros.

E é justamente nossa maior dependência da internet que faz com que a importância da segurança e privacidade aumente. Como usuários, devemos exigir e utilizar serviços e plataformas que não comprometam nossa segurança e protejam nossa privacidade. Como profissionais de segurança e privacidade, devemos trabalhar para que os serviços, plataformas, aplicações, aplicativos e sistemas sejam construídos de forma a não potencializar as ameaças existentes na internet, as quais podem resultar em prejuízos que vão além do aborrecimento, indo para comprometimento de reputação, perdas financeiras e que podem chegar até mesmo ao comprometimento da saúde e vida, nos casos que envolvem a internet das coisas ou *Internet of Things, IoT*.

A segurança na internet é um dos assuntos abordados nesta unidade, com o entendimento dos aspectos envolvidos nas transações *web*, que devem ser protegidos, principalmente dos dados que trafegam pela internet. Uma vez que seus dados chegam ao destinatário, eles devem ser protegidos para que não vazem ou sejam utilizados de forma ilícita. Os dados dos usuários são cada vez mais valiosos, já que podem ser utilizados para que identidades digitais das vítimas sejam criadas de uma forma ilegítima ou usados diretamente para transações ilegais, no caso de dados bancários, por exemplo. E há diversos tipos de golpes na internet que podem levar ao acesso ilegal a dados dos usuários. Alguns desses principais golpes serão discutidos, bem como o uso seguro de internet, e as questões para a privacidade na *Web*.

O acesso à internet é feito com o uso de dispositivos e um dos principais é o dispositivo móvel, com os smartphones, representando grande parte dos acessos à rede. Iremos discutir o que isso representa, sob o

ponto de vista de segurança e privacidade, analisando principais ameaças, ataques e mecanismos de defesa em dispositivos móveis, incluindo a camada de aplicação e o uso de antivírus para a proteção. Outro ponto importante é a proteção dos usuários dos dispositivos móveis, que estão sujeitos a ataques de engenharia social, que podem resultar no acesso às informações pessoais.

O acesso à internet é feito com o uso de dispositivos e um dos principais é o dispositivo móvel, com os *smartphones*, representando grande parte dos acessos à rede. Iremos discutir o que isso representa, sob o ponto de vista de segurança e privacidade, analisando principais ameaças, ataques e mecanismos de defesa em dispositivos móveis, incluindo a camada de aplicação e o uso de antivírus para a proteção. Outro ponto importante é a proteção dos usuários dos dispositivos móveis, que estão sujeitos a ataques de engenharia social, que podem resultar no acesso às informações pessoais.

Após o entendimento dos principais ataques na internet e as particularidades da segurança em dispositivos móveis, abordaremos uma das principais atividades de profissionais de segurança da informação, que leva ao entendimento do ambiente, dos componentes ou ativos deste ambiente e das vulnerabilidades que podem ser exploradas em ataques. Já vimos que um incidente de segurança é resultado da exploração de vulnerabilidades de ativos por agentes de ameaça, fazendo com que uma ameaça se concretize. Uma das principais formas de se evitar incidentes de segurança é, assim, identificar e tratar as vulnerabilidades dos diferentes ativos do ambiente. Há uma série de métodos e formas de se trabalhar com as vulnerabilidades, incluindo testes de intrusão ou *pentests* e análises de vulnerabilidades. E, dependendo da informação disponível para realizar os testes ou análises, o trabalho pode ser definido como *blackbox* ou *whitebox*. Teremos uma sessão inteira para aprofundar este tema.

Vamos iniciar os estudos pela segurança na internet.

Bons estudos!

PRATICAR PARA APRENDER

Olá, nesta seção, discutiremos aspectos importantes de segurança e privacidade na internet, focando nas transações *web*. Neste contexto, há três ambientes que podem ser explorados pelos agentes de ameaça e que, portanto, precisam ser protegidos: o ambiente do usuário, o ambiente do provedor de internet e o ambiente do provedor de serviços. Os dados e as informações podem ser modificados, furtados ou destruídos nestes três ambientes.

Os controles de segurança, que são técnicos, físicos ou processuais, podem ser implementados na sua empresa. Porém, as transações *web* podem chegar à empresa já sem a autenticidade ou integridade, como no caso das transações fraudulentas com uso de identidades furtadas ou uso de cartões de créditos de terceiros.

Desta forma, além de proteger o perímetro de sua empresa, é preciso atuar também com os seus clientes, que podem ser vítimas de ataques como o *phishing*, que leva à instalação de *malwares* que furtam, modificam informações ou levam a sites falsos, onde as vítimas inserem seus dados e informações, os quais são furtados e utilizados em atividades criminosas.

Discutiremos também como os usuários podem ser atingidos por golpes na internet e como eles podem fazer o uso seguro dessa ferramenta, cuidando de sua privacidade.

Você foi contratado como analista de segurança e privacidade de um inovador site de comércio online em que pequenos negócios são conectados com os consumidores em uma plataforma digital baseada no uso de inteligência artificial. A sua função é essencial para a empresa, e você participa de todas as decisões sobre a evolução da plataforma. Há as questões envolvidas com o desenvolvimento seguro, para que vulnerabilidades não sejam inseridas. Há ainda as questões de segurança e privacidade envolvidas com o uso de provedor de nuvem. E, como a empresa trabalha com inteligência artificial, há necessidade de fazer o desenvolvimento utilizando bases de dados que não interfiram na privacidade dos clientes.

Além da segurança da informação da plataforma da empresa, que está hospedada em um provedor em nuvem na Europa, você tem três preocupações principais:

1. Como diminuir as possíveis fraudes cometidas por usuários falsos que se passam por clientes, com uso de identidades falsas ou uso de recursos financeiros ilícitos;.
2. Como diminuir as possíveis fraudes cometidas por pequenos negócios falsos, que podem não cumprir os compromissos comerciais estabelecidos com os clientes que utilizam a plataforma digital;.
3. Como proteger os dados pessoais dos clientes principalmente contra vazamentos, que pode levar a sanções previstas na LGPD.

Você deverá fazer um planejamento e preparar um relatório com uma lista de aspectos que devem ser considerados pela empresa para a definição de uma estratégia de segurança e privacidade. O foco deste planejamento deve ser a segurança na internet, com o seu direcionamento quanto à segurança em transações *web*, considerando

o ambiente de negócios da empresa e as três preocupações principais que você tem: fraudes cometidas por usuários falsos, fraudes cometidas por pequenos negócios falsos e como proteger os dados pessoais dos clientes.

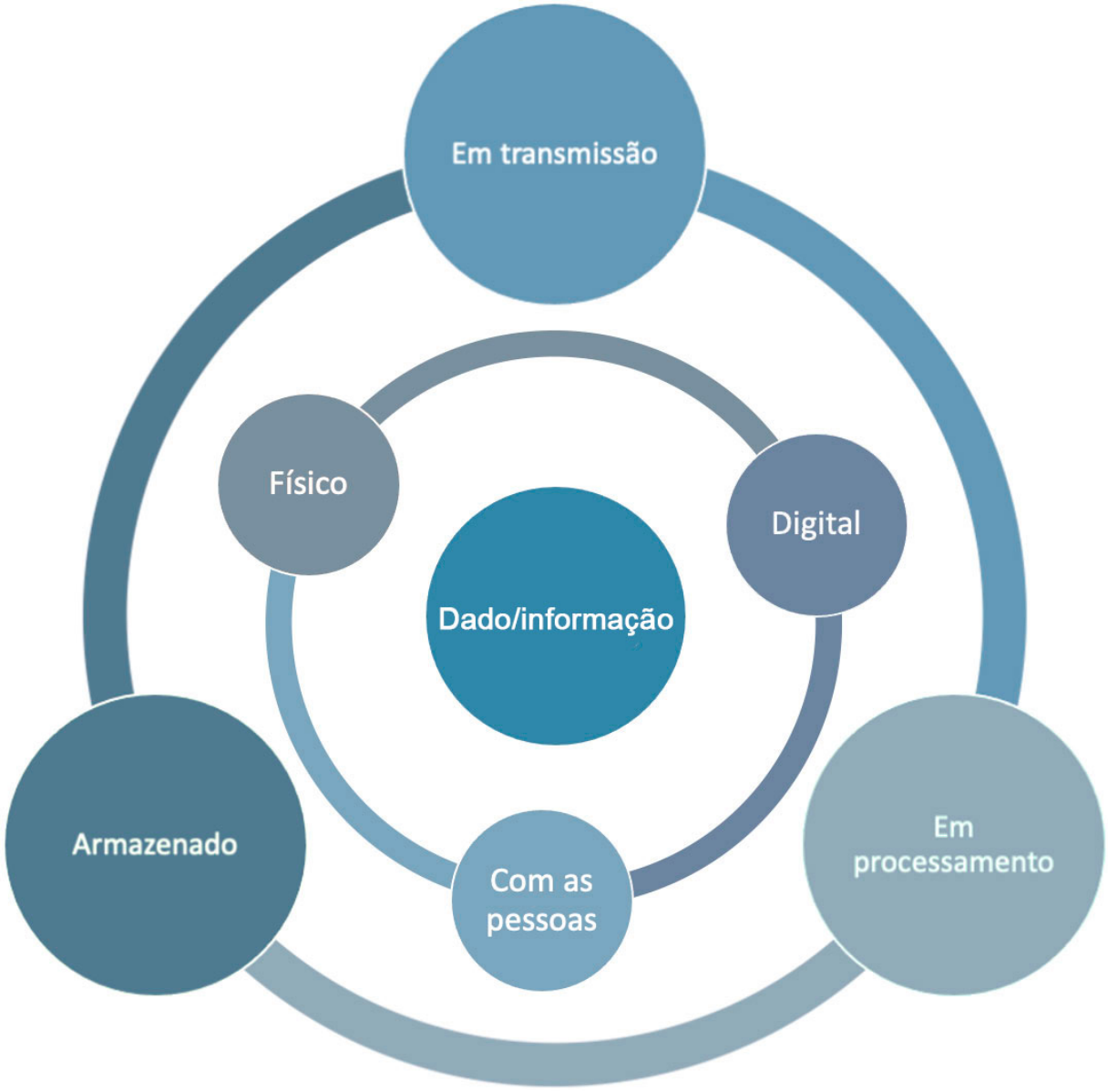
O conteúdo desta seção é importante e útil para todos, desde o ponto de vista de usuário, empresa, clientes e fornecedores. E você, como profissional de segurança e privacidade, deve adotar estes conceitos para trabalhar o treinamento e a conscientização de todos, fazendo com que a empresa tenha o nível de segurança e privacidade elevado.

Uma cultura forte em segurança e privacidade é essencial para todos os profissionais da área.

CONCEITO-CHAVE

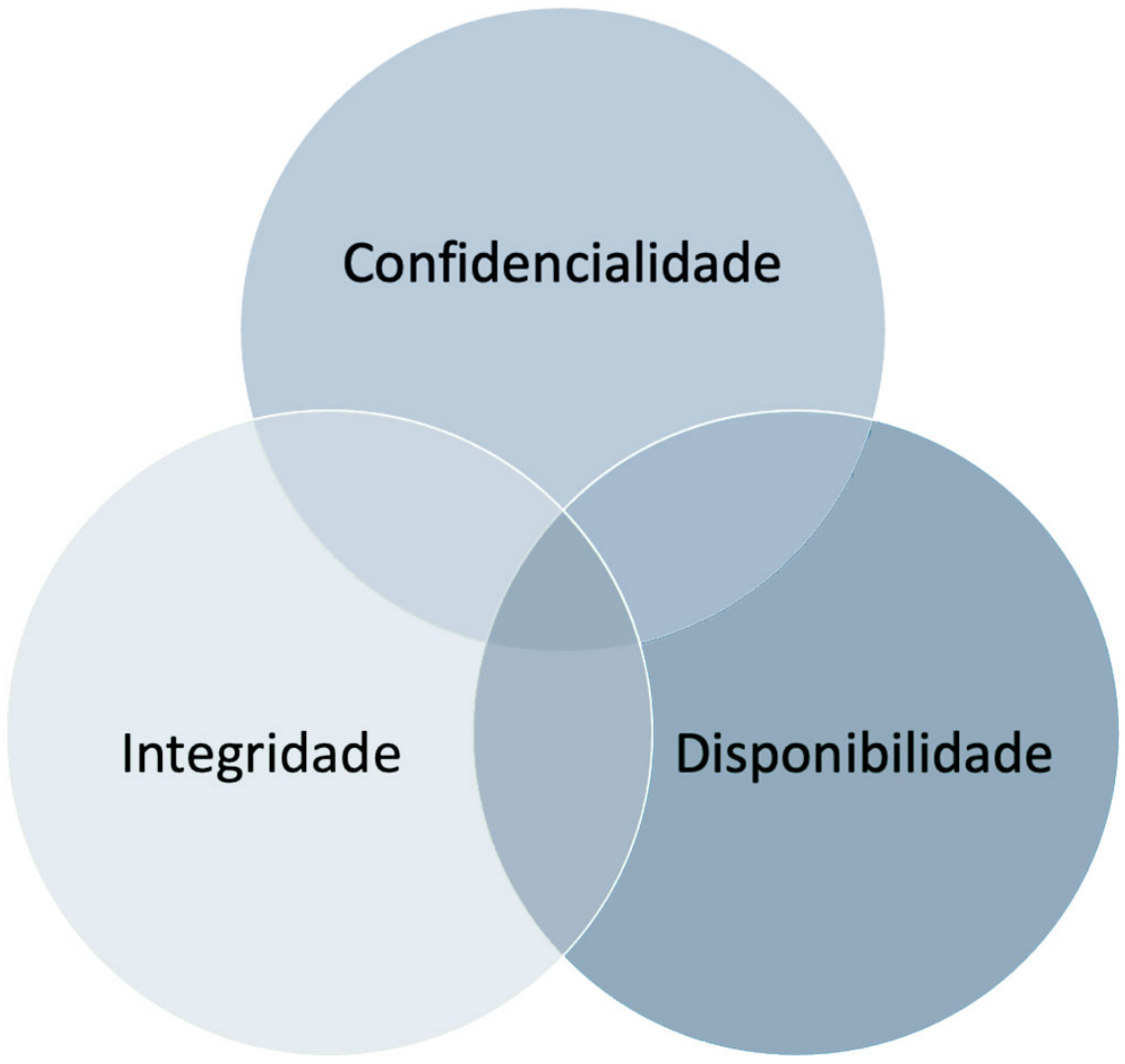
A segurança e privacidade na internet passam pelo entendimento de diferentes elementos que envolvem o que deve ser protegido e os componentes ou ativos de um ambiente que podem ser explorados em ataques. Vamos relembrar estes elementos para seguirmos adiante. A Figura 3.1 ilustra que o dado ou a informação existe na forma digital como nos servidores de banco de dados, na forma física como em papel ou na cabeça das pessoas. Além disso, os dados digitais estão em diferentes estados: em transmissão, em processamento ou armazenados. O escopo da segurança da informação abrange diferentes formas e estados dos dados e das informações. E a proteção é para que sejam preservadas a tríade CID, que corresponde à confidencialidade, integridade e disponibilidade (Figura 3.2) dos dados e informações, em todas as suas formas e todos os estados.

Figura 3.1 | Formas e estados do dado e informação



Fonte: elaborada pelo autor.

Figura 3.2 | Tríade CID: confidencialidade, integridade e disponibilidade



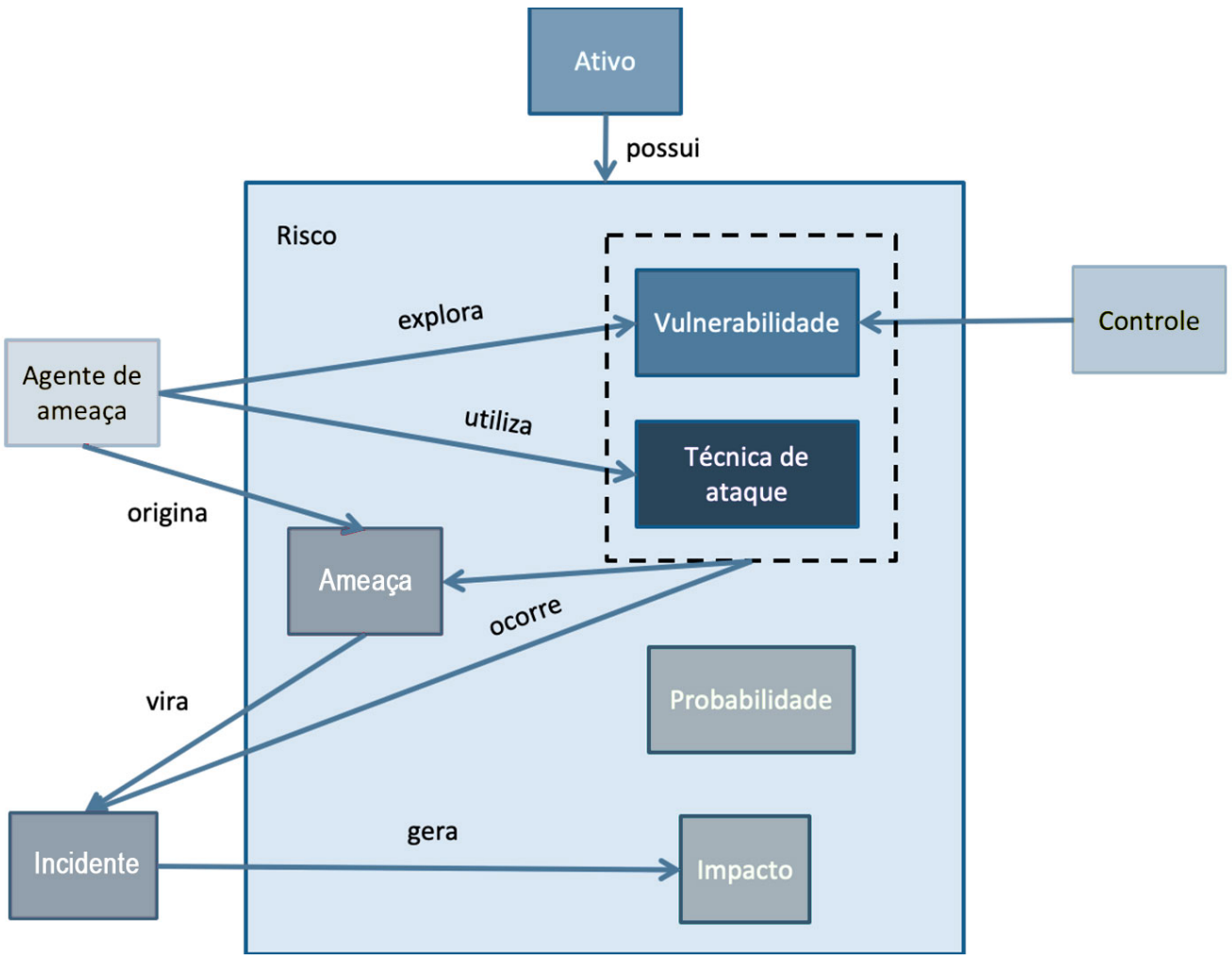
Fonte: elaborada pelo autor.

Outros elementos importantes são aqueles do risco, que podem ser vistos na Figura 3.3. Um risco é a probabilidade de um agente de ameaça explorar vulnerabilidade de um ativo utilizando uma técnica de

Ver anotações 0

ataque, o que faz com que uma ameaça se torne um incidente de segurança, o que resulta em impactos para a organização. Os controles de segurança são implementados para tratar as vulnerabilidades específicas daquele ativo.

Figura 3.3 | Elementos do risco



Fonte: elaborada pelo autor.

Todos esses elementos fazem parte do entendimento da segurança na internet. As transações web, que partem dos usuários que utilizam seus dispositivos a partir de algum local em que há uma conexão com a internet, passam por variados componentes até chegar à loja virtual, ao serviço do governo ou ao banco. Neste caminho, os agentes de ameaça estão à espreita em busca de oportunidades para roubar os dados pessoais, dados das transações web e as identidades digitais. Além da exploração de vulnerabilidades, estes agentes de ameaça buscam os golpes na internet para o mesmo fim, isto é, ter acesso a informações valiosas (OLIVEIRA, 2017).

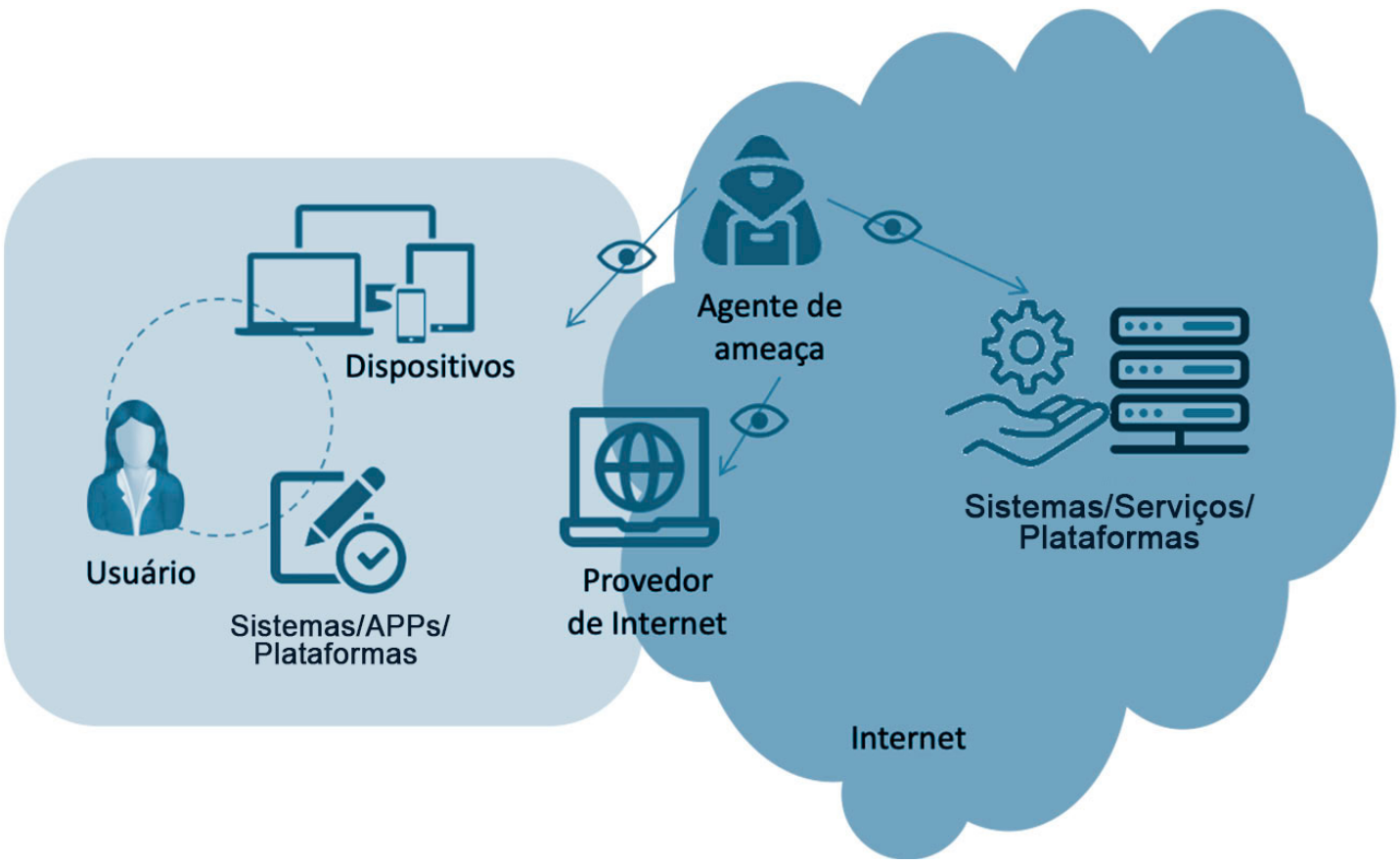
A Figura 3.4 ilustra esta dinâmica da segurança na internet, com o agente de ameaça buscando oportunidades em três ambientes:

- No ambiente do usuário.

- No ambiente de Internet que inclui o provedor de internet.
- No ambiente dos provedores de serviços, sistemas e plataformas.

Há a necessidade de segurança pelo usuário, que deve proteger o seu ambiente composto por ele próprio, os dispositivos e os sistemas, aplicativos e plataformas que ele instala em seus dispositivos. Há ainda a necessidade de segurança pelo provedor de internet, que além do canal de comunicação que dá o acesso à internet provê o acesso a serviços fundamentais como o *Domain Name Service (*DNS), o qual em caso de comprometimento pode levar os usuários a sites falsos. E há a necessidade de segurança pelos provedores de sistemas, serviços e plataformas, compostos pelas empresas que incluem bancos, comércio eletrônico, serviços de governo, serviços de saúde, comunicação, entre outros.

Figura 3.4 | Segurança na internet



Fonte: elaborada pelo autor.

SEGURANÇA EM TRANSAÇÕES *WEB*

As transações *web*, realizadas pela internet, envolvem uma série de questões de segurança que partem do usuário e chegam ao provedor de serviços, como um banco, passando pelo provedor de internet.

Uma transação *web* pode ser uma compra online, uma transação bancária, a realização de algum serviço governamental ou até mesmo uma postagem em uma rede social.

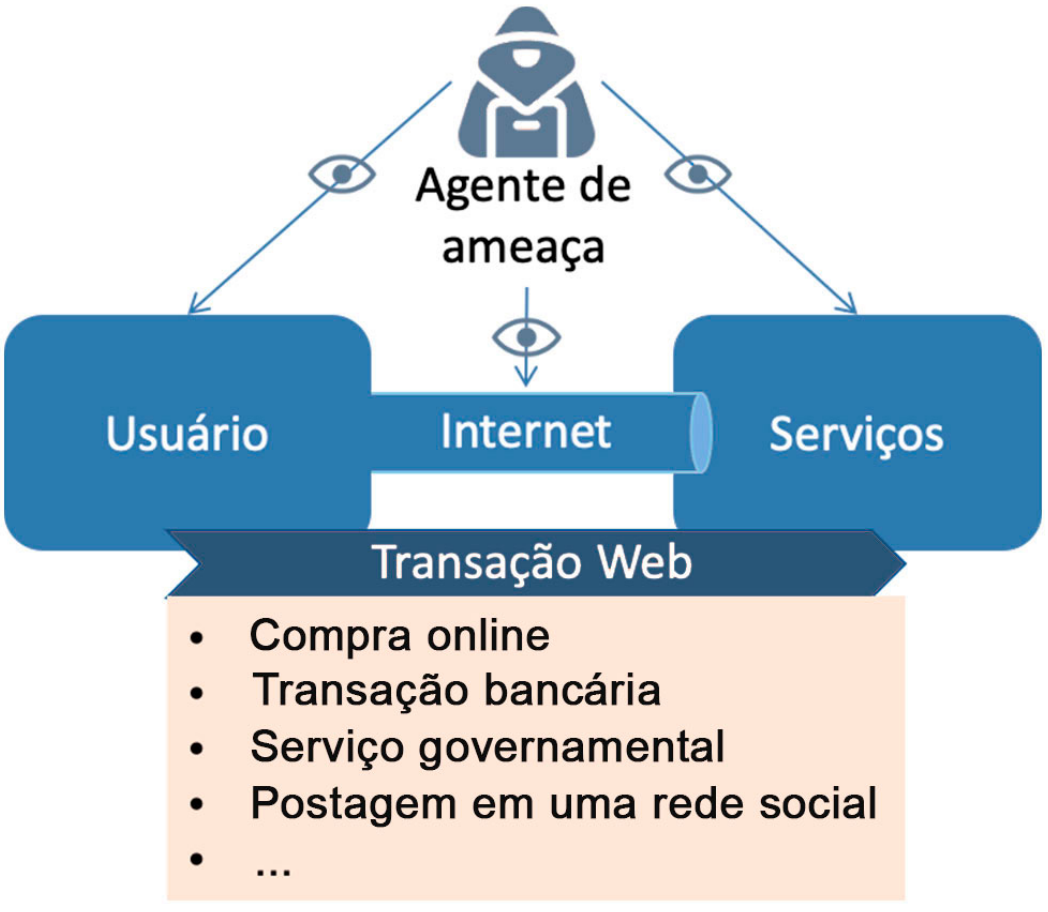
E as transações podem envolver diferentes tipos de dados ou informações: dados pessoais, dados financeiros ou dados confidenciais, que podem sofrer modificações, vazamentos ou destruições, afetando, respectivamente, a integridade, confidencialidade e disponibilidade.

> **REFLITA**
>
> Uma transação possui diferentes significados, dependendo do contexto. No seu conceito mais amplo, uma transação significa a troca de bens. Já no contexto da tecnologia, no caso de banco de dados, uma transação significa uma operação ou uma unidade de trabalho executado de uma forma coerente e confiável, independente de outras transações (CONCEITOS, 2020). E, com os ataques cibernéticos, as transações podem ser manipuladas, vazadas ou removidas antes, durante ou após chegarem ao seu destino.

A segurança em transações web passa pela proteção dos três ambientes, como pode ser visto na Figura 3.5:

- Ambiente do usuário, composto pelo próprio usuário, seus dispositivos e os sistemas, aplicativos e plataformas instaladas.
- Ambiente de internet, composto pela comunicação e o provedor de internet.
- Ambiente do serviço, sistema, plataforma ou aplicação, composto pela empresa que presta o serviço que está sendo acessado pelo usuário.

Figura 3.5 | Segurança em transações web



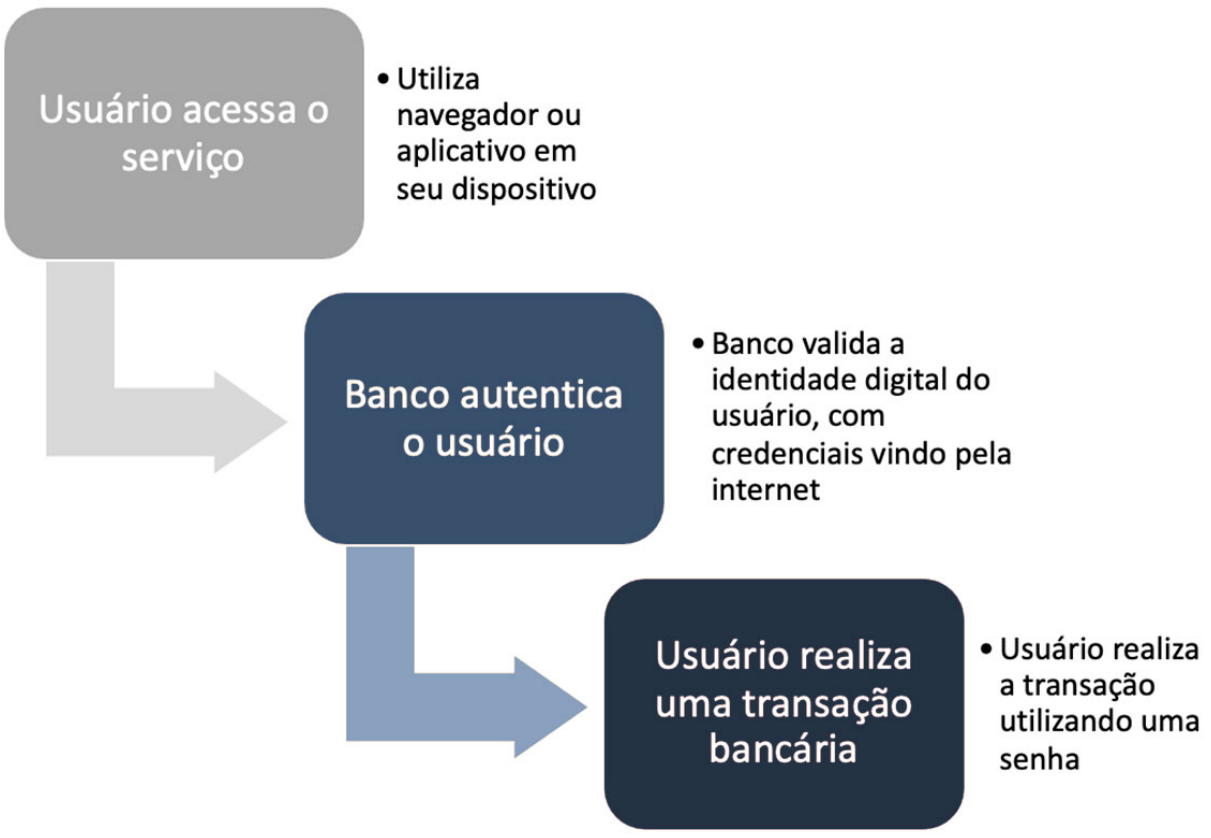
Fonte: elaborada pelo autor.

Os dados e as informações existem em seus três estados (em processamento, em transmissão e em armazenamento) e podem sofrer ataques em qualquer ponto de um dos três ambientes. Estes pontos de ataques são representados por ativos humanos, físicos ou tecnológicos. Por exemplo: um agente de ameaça pode atacar o próprio usuário buscando a engenharia social para a instalação de um *malware*. Ou o agente de ameaça pode monitorar o tráfego de um provedor de internet em busca de dados e informações. Além dessas possibilidades, o agente de ameaça pode explorar vulnerabilidades da aplicação do provedor de serviços para o acesso não autorizado aos dados das transações.

Em um exemplo de transação bancária, o fluxo simplificado pode ser visto na Figura 3.6. O usuário utiliza seu dispositivo e acessa a instituição financeira, o banco, por seu navegador ou pelo uso de uma aplicação instalada em seu dispositivo. O usuário então se identifica utilizando uma identidade digital como o seu CPF, número de agência e conta ou nome de usuário. A validação da identidade, ou autenticação do usuário, é feita pelo uso de uma senha. Uma vez dentro do serviço do

banco após a autenticação, o usuário pode fazer uma transação bancária, como uma transferência ou um pagamento de conta. Essa transação exige uma autenticação adicional, como o uso da senha do cartão bancário. E toda essa comunicação entre o usuário, a partir do navegador ou aplicativo, chega ao servidor do banco, passando pela internet.

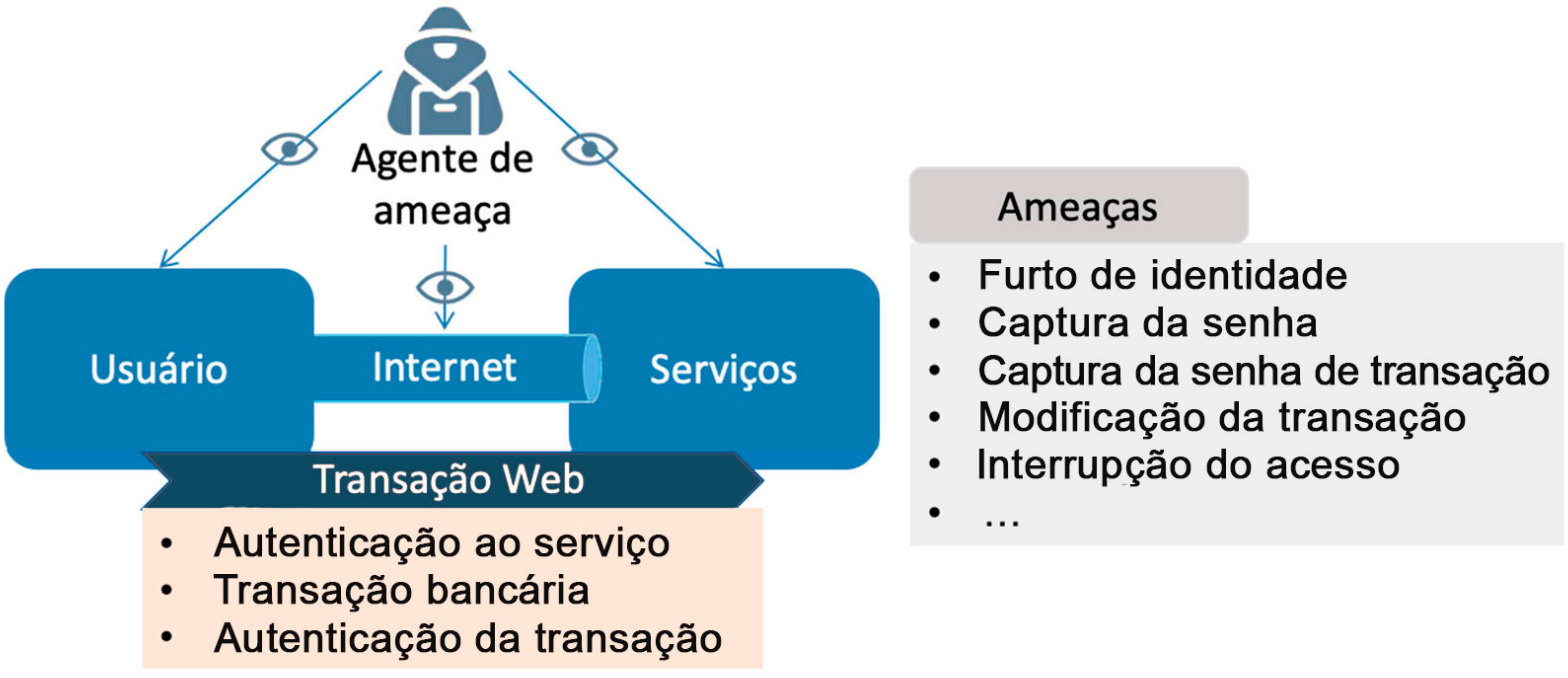
Figura 3.6 | Exemplo de transação *web* em bancos



Fonte: elaborada pelo autor.

As ameaças, neste exemplo, são o furto de identidade, a captura da senha, a captura da senha de transação, a modificação da transação e a interrupção do acesso, que podem afetar a autenticação ao serviço, a transação bancária e a autenticação da transação (Figura 3.7). Elas podem ocorrer em qualquer um dos três ambientes, porém de uma forma diferente, o que leva à necessidade de controles de segurança diferentes, que afetam também as responsabilidades.

Figura 3.7 | Ameaças no exemplo de transação *web* em bancos



Fonte: elaborada pelo autor.

Os três ambientes precisam ser protegidos. Os dados de autenticação ao serviço, da transação bancária e da autenticação da transação podem ser capturados, modificados ou removidos de diferentes formas. No **ambiente do usuário**, as transações *web* exigem segurança porque malwares podem capturar e modificar dados a partir da origem no próprio usuário. Neste caso, a transação chega ao provedor de serviços, como o banco, já de uma forma ilegítima, seja pela modificação da transação ou pelo furto de identidade. O provedor de serviços, assim, além de ter de proteger o seu próprio ambiente, tem o desafio de receber uma transação vindo de um criminoso, que furtou a identidade do usuário verdadeiro.

EXEMPLIFICANDO

Os bancos têm investido muito em comunicação e campanhas para os seus clientes, para que não sejam vítimas de fraudes que levam ao furto de identidades. Além disso, utilizam mecanismos de segurança como autenticação de duplo fator e sistemas antifraude (CARVALHO, 2018). Com a autenticação de duplo fator, é necessário, além da senha, um código único que é enviado para o dispositivo móvel do usuário, de uma forma que, no caso de furto de credencial do usuário, ainda é necessário o código enviado para o dispositivo móvel para o acesso ou a transação bancária.

Outro fator de autenticação, utilizado normalmente para confirmar as transações, é a biometria. Já o sistema antifraude analisa diferentes parâmetros das transações com base em perfil de usuário para tentar identificar se é realmente o usuário legítimo que está fazendo a transação.

No **ambiente de internet**, em que o agente de ameaça pode capturar ou modificar as transações web, é importante que elas sejam realizadas com o uso de um canal seguro, que deve ser provido pelo provedor de serviços, como o banco. As conexões web podem ser protegidas com o uso de protocolos de segurança como o *Hyper Text Transfer Protocol Secure* (HTTPS), que foi visto na Unidade 1 da disciplina. O HTTPS possibilita o uso do HTTP sobre uma sessão *Secured Socket Layer* (SSL) ou *Transport Layer Security* (TLS), com a criação de um túnel seguro por onde trafegam as informações. Além de garantir a confidencialidade (dados cifrados com chave simétrica de sessão), eles podem visar também a integridade dos dados (uso de *Message Authentication Code*, MAC) e a autenticidade das partes (as entidades podem ser autenticadas com o uso de criptografia de chave pública).

Já no **ambiente do provedor de serviços**, como no caso de bancos, o ambiente pode ser atacado em qualquer um dos componentes, incluindo as aplicações, os servidores de aplicação, os sistemas operacionais, as máquinas virtuais, os bancos de dados. Toda a estratégia de segurança da informação corporativa deve ser seguida pelos provedores de serviços, incluindo as ações de segurança e privacidade com os processos e as pessoas. É importante que o profissional de segurança e privacidade considere que os ataques podem ter origem externa, mas também interna.

ASSIMILE

A segurança em transações web envolve o entendimento das ameaças que existem em três ambientes: do usuário, da internet e do provedor de serviços. Uma transação web tem a

origem no usuário, que utiliza dispositivos e aplicações, que chegam até os servidores do provedor de serviços, como os bancos, pela internet. Há ameaças neste caminho também quando as transações chegam ao provedor de serviços. Os dados e as informações passam por diferentes estados neste fluxo das transações web, sendo processados, transmitidos e armazenados.

GOLPES NA INTERNET

As ameaças existentes nas transações web envolvem os usuários, os provedores de internet e os provedores de serviços. Um dos grandes desafios dos profissionais de segurança e privacidade é fazer com que o equilíbrio da segurança possa ser estabelecido, o que é difícil para os provedores de serviços, que vêm implementando um conjunto de controles de segurança para minimizar os efeitos negativos de um ambiente de usuário contaminado. Esta contaminação faz com que uma transação já chegue de uma forma insegura, como no caso de um criminoso se passando pelo usuário legítimo.

E a contaminação do usuário é um ponto essencial para ser tratado, já que leva ao furto de identidades e a transações fraudulentas, como pagamento de boletos falsos, levando a prejuízos tanto para o usuário quanto para as empresas.

EXEMPLIFICANDO

Bolware é um tipo de ataque em que os usuários são vítimas de um vírus que altera os boletos. Quando uma operação de pagamento está sendo realizada, o *malware* intercepta a transmissão e troca os dados do boleto legítimo. O sistema do banco acaba então recebendo e processando as informações do boleto falso (ALECRIM, 2014).

Os golpes na internet, assim, visam explorar os usuários, com uso de técnicas de engenharia social que levam à instalação de *malwares*, ao direcionamento para *sites* falsos e ao envio de dados sensíveis para criminosos. O resultado é um conjunto de atividades maliciosas que incluem o furto de identidades para criação de contas fraudulentas em serviços *online* e bancos, a realização de transações ilícitas, o envio de mensagens falsas, o acesso a serviços variados por terceiros, entre outras atividades possíveis a partir das credenciais das vítimas ou dados sensíveis.

O CERT.br (2020) lista alguns dos principais golpes aplicados na internet (Figura 3.8):

- **Furto de identidade**, com o criminoso tentando a se passar pelo usuário real, podendo criar contas em seu nome, realizando transações indevidas ou enviando mensagens ou postagens em seu nome.
- **Fraude de antecipação de recursos**, em que o golpista procura induzir a vítima a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício. Exemplos são o golpe da Nigéria, e outros que envolvem loteria internacional, crédito fácil, doação de animais, oferta de emprego e noiva russa. Outro golpe é o do WhatsApp, em que o golpista obtém o acesso à conta da vítima se passando por um funcionário de uma empresa que solicita um código de reinicialização (que na realidade é do WhatsApp) e a partir dessa transferência das credenciais para o golpista, os contatos da vítima passam a receber solicitações de depósitos para pagamento de uma dívida, que são feitas na conta do golpista.
- ***Phishing* ou *scam***, em que o golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Este golpe explora a atenção, curiosidade, caridade, medo ou possibilidade de obtenção de

vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou *site* popular. Envolve a possibilidade de inscrição em serviços de proteção de crédito, ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas falsas em que entregam suas credenciais, senhas ou informações sensíveis, além da instalação de códigos maliciosos.

- ***Pharming***, em que a vítima tem a sua navegação redirecionada por meio de alterações no serviço de *Domain Name System* (DNS), que ao invés do site correto, leva a um site falso. Essa alteração pode ser feita no dispositivo do usuário, ou no provedor de internet;

- **Golpes de comércio eletrônico**, em que são exploradas as relações de confiança existentes entre partes envolvidas em uma transação comercial. Envolvem a criação de site de comércio eletrônico fraudulento e o uso *sites* de compras coletivas ou de leilão, em que obtém os recursos, porém não cumprem os acordos comerciais, como uma venda em que o dinheiro é obtido sem a entrega dos produtos.

- **Boato ou *hoax***, em que conteúdos alarmantes ou falsos levam a tentativas de golpes, como correntes e pirâmides, além de poder conter códigos maliciosos, espalhar desinformação pela internet e comprometer a credibilidade e reputação de pessoas e empresas.

Figura 3.8 | Principais golpes na internet

Fonte: elaborada pelo autor.

DICA

Uma fonte de informações sobre fraudes, golpes, burlas, lavagem de dinheiro, corrupção e outros perigos que existem na vida privada, na internet, no setor público e no mundo financeiro e dos negócios é o Monitor das Fraudes (MONITOR, 2020). Outra fonte é o Catálogo de Fraudes da RNP (RNP, 2020), que alerta a comunidade sobre os principais golpes em circulação na internet.

As principais ações para a proteção contra os golpes aplicados na internet são a notificação para a organização envolvida a fim de se tomar as medidas cabíveis e a busca constante de informação sobre o assunto. Em alguns casos, ataques de negação de serviço coordenados (*Distributed Denial of Service*, DDoS) são utilizados em conjunto, o que tornam serviços como o comércio eletrônico das empresas indisponíveis e tornam as fraudes mais plausíveis.

USO SEGURO DE INTERNET

O uso seguro de internet pelos usuários é parte fundamental da segurança das empresas. No caso dos bancos, por exemplo, uma transação pode chegar à instituição já de uma forma fraudulenta, seja pelo furto de identidade de um cliente legítimo, seja pela alteração de transações, como no caso de boletos bancários.

Assim, um papel importante do profissional de segurança é considerar os usuários e clientes como um dos principais ativos a serem protegidos, com o uso constante de treinamento e conscientização.

O uso seguro de internet pelos usuários envolve, principalmente, dois pontos principais:

- Como saber se um *site* é seguro?
    - A empresa deve configurar o HTTPS/TLS/SSL e o usuário deve verificar as informações do certificado digital utilizado para validar a empresa e o site, se possuem as informações correspondentes.
- Como saber se um *site* é falso?
    - A empresa deve configurar o HTTPS/TLS/SSL e o usuário deve verificar o endereço ou URL que está sendo acessado, com atenção, já que *sites* falsos costumam inserir caracteres especiais ou modificações sutis do endereço real. Endereços falsos são enviados a vítimas em *e-mails*, ou SMS, de modo que os endereços de sites devem ser digitados diretamente no navegador.

Algumas das principais recomendações para usuários, que devem ser incluídas em treinamentos e campanhas de conscientização, são (CARVALHO, 2018):

1. Não acesse *sites* a partir de computadores compartilhados, que podem conter *malwares* que capturam os dados inseridos, como dados sensíveis ou credenciais de acessos.

2. Não acesse *sites* a partir de redes *wi-fi* públicas, que podem direcionar a *sites* falsos ou fazem a conexão com sites, com a captura dos dados trafegados.

3. Mantenha o antivírus do dispositivo sempre atualizado, para que seus dispositivos não sejam contaminados com *malwares*.

4. Digite o endereço do site no navegador, para evitar sites falsos a partir de *links* recebidos por *e-mails* ou SMS.

5. Habilite a verificação em duas etapas ou o duplo fator de autenticação, para evitar acessos indevidos às contas em caso de furto de identidade ou credenciais de acesso.

6. Não clique em *links* recebidos por *e-mail* ou SMS, para evitar ser direcionado a *sites* falsos que buscam obter seus dados sensíveis e credenciais de acesso.

7. Cuidado ao usar extensões no navegador, que podem instalar *malware*s em seus dispositivos.

PRIVACIDADE NA *WEB*

A privacidade na *web* possui visões a serem consideradas. De um lado, há o rastreamento do que as pessoas fazem na *web*, como os *cookies*. Do outro, há a divulgação espontânea de informações pessoais em redes sociais, que podem resultar em crimes que transcendem o digital e podem afetar diretamente as pessoas com fraudes e crimes diversos. E, com a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2020), todos devem preservar a privacidade e a proteção de dados pessoais.

> **REFLITA**
>
> A privacidade é um direito fundamental da pessoa natural, e diz respeito à proteção de dados pessoais, que, segundo a LGPD, é a informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2020). Dados e informações corporativos podem ser considerados sigilosos e

Ver anotações

> confidenciais, dependendo dos níveis de classificação da informação, e não possuem relação direta com a privacidade. Alguns dados pessoais, no entanto, podem existir em documentos sigilosos ou confidenciais.

O rastreamento do que as pessoas fazem na *web* corresponde a dados que identificam uma pessoa e do mesmo modo devem ser protegidos segundo a LGPD. A privacidade na web, neste contexto, faz com que os dados pessoais devam ser tratados pelas empresas com toda a segurança necessária. Os usuários, que são os donos ou titulares dos seus dados, devem ter o total conhecimento sobre o que está sendo tratado e como estão sendo protegidos pelas organizações. A privacidade na *web*, assim, não significa que as organizações não podem tratar os dados pessoais, mas sim que os usuários têm direitos sobre estes dados e eles devem ser protegidos com a segurança da informação. Um dos mecanismos para que a privacidade funcione é o consentimento, que pode ser de acordo com uma base legal (BARROS, 2020).

De uma forma geral, o usuário, ao acessar um *site*, deve saber que um *cookie* está ativo, se for o caso, e deve aceitar o seu uso. Já no momento de inserir dados pessoais, o usuário deve ter acesso a um aviso de privacidade, que diz quais dados e a finalidade da coleta, o compartilhamento com outras entidades e a forma como eles serão protegidos. Após o aceite do usuário, a empresa deve proteger os dados coletados para evitar vazamentos. Em caso de vazamento ou a falta de aviso de privacidade, a empresa está sujeita às sanções da LGPD, que podem chegar à multa e à paralização das operações. O usuário tem uma série de direitos, como o de consulta sobre quais dados estão de posse da empresa, e de solicitação de remoção, que deve ser feito em caso de não haver uma exigência legal para que eles sejam preservados.

Assim, a privacidade na *web* tem elementos que exigem uma série de atividades do profissional de segurança e privacidade. A LGDP reforça a necessidade dos controles de segurança, já que um vazamento pode resultar em sanções previstas na lei. As questões de privacidade e proteção de dados pessoais devem fazer parte das atividades dos profissionais de segurança da informação.

Ver anotações

SAIBA MAIS

O CERT.br (2020) faz uma série de recomendações importantes para a privacidade. Para a proteção da sua vida profissional, algumas recomendações são:

- Cuide da sua imagem profissional. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode atrapalhar um processo seletivo que você venha a participar (muitas empresas consultam as redes sociais à procura de informações sobre os candidatos, antes de contratá-los);
- Verifique se sua empresa tem um código de conduta e procure estar ciente dele. Observe principalmente as regras relacionadas ao uso de recursos e divulgação de informações;
- Evite divulgar detalhes sobre o seu trabalho, pois isto pode beneficiar empresas concorrentes e colocar em risco o seu emprego;
- Preserve a imagem da sua empresa. Antes de divulgar uma informação, procure avaliar se, de alguma forma, ela pode prejudicar a imagem e os negócios da empresa e, indiretamente, você mesmo;
- Proteja seu emprego. Sua rede de contatos pode conter pessoas do círculo profissional que podem não gostar de saber que, por exemplo, a causa do seu cansaço ou da

sua ausência é aquela festa que você foi e sobre a qual publicou diversas fotos;

- Use redes sociais ou círculos distintos para fins específicos. Você pode usar, por exemplo, uma rede social para amigos e outra para assuntos profissionais ou separar seus contatos em diferentes grupos, de forma a tentar restringir as informações de acordo com os diferentes tipos de pessoas com os quais você se relaciona.

PESQUISE MAIS

Atacantes podem ser internos e externos e têm motivações diferentes. Eles executam uma série de ataques, os quais exigem que as organizações implementem seus controles de segurança. O livro *Tópicos de segurança da informação*, de OLIVEIRA (2017), no capítulo 6, sobre “Principais Ataques Virtuais e suas Contramedidas”, cita os perfis de atacantes, e os principais ataques e contramedidas. (OLIVEIRA, 2017).

OLIVEIRA, R. C. Q. **Tópicos de segurança da informação**. São Paulo: Editora Senac São Paulo, 2017.

Chegamos ao final desta seção, que tratou de aspectos da segurança na internet, que envolve usuários, provedores de internet e provedores de serviços. As transações *web* precisam de segurança e, muitas vezes as empresas dependem da segurança do ambiente dos usuários, que podem ter suas identidades furtadas ou serem fonte de transações fraudulentas. O treinamento e a conscientização dos usuários são essenciais, para que recebam recomendações para não cair em golpes na internet e para que façam uso seguro da internet. A privacidade na web ganhou ainda mais importância com a LGPD, que estabelece direitos para os usuários, os quais têm o direito fundamental à privacidade. Os dados pessoais devem ser protegidos e os direitos dos usuários, incluindo a transparência relacionada ao tratamento dos dados, devem ser cumpridos.

FAÇA VALER A PENA

Questão 1

Um dos principais ataques contra usuários explora atenção, curiosidade, caridade, medo ou possibilidade de obtenção de vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou site popular. Envolve a possibilidade de inscrição em serviços de proteção de crédito ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas falsas onde entregam suas credenciais, senhas ou informações sensíveis, e podem instalar no dispositivo do usuário códigos maliciosos.

Assinale a alternativa que apresenta o tipo de ataque que explora diretamente os usuários.

a. *Phishing*.

b. *Pharming*.

c. *Malware*

d. DDoS.

e. *Firewall*.

Questão 2

Em ataques de *phishing*, o golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Uma das principais técnicas é o envio de uma mensagem de e-mail ou um SMS com um *link* para um assunto de interesse da vítima.

Assinale a alternativa que contém uma forma em que o usuário pode se proteger contra ataques de *phishing*.

a. Não há proteção contra este ataque.

b. Instalando um *firewall.*

c. Instalando um antimalware.

d. Não clicando em links recebidos.

e. Atacando o remetente.

Questão 3

Você trabalha em uma empresa que comercializa materiais de construção pela internet. Ultimamente a empresa tem recebido muitos pedidos fraudulentos, os quais têm gerado um grande prejuízo. Estes pedidos são feitos por clientes antigos, que depois negam os pedidos, já que nem receberam os produtos. Já outros clientes entram em contato porque estranham transações em seus cartões de crédito na loja, sem que tenham feito pedidos.

Você acredita que um ataque cibernético está levando a essas fraudes. O acesso ao serviço é feito pelos clientes usando HTTPS. E, além do IPS não ter emitido nenhum alerta, você já analisou os logs dos servidores, não detectando nenhum acesso suspeito, principalmente no banco de dados. O fato pode estar ocorrendo pois:

a. sua empresa foi *hackeada* e os rastros foram apagados.

b. os usuários estão sendo contaminados com uma nova campanha de *phishing*.

c. os *hackers* estão invadindo bancos e roubando números de cartões de crédito.

Ver anotações

d. os clientes estão compartilhando senhas com o público, que fazem compras usando contas de terceiros.

e. os *hackers* estão capturando as informações de sua empresa na internet.

REFERÊNCIAS

ALECRIM, E. RSA: malware que altera boletos bancários pode ter causado prejuízo de R$ 8,5 bilhões. **Tecnoblog**, Antivírus e Segurança, 2 jul. 2014. Disponível em: https://bit.ly/2PjVEal. Acesso em: 20 dez. 2020.

BARROS, M. 10 Bases Legais da LGPD: Quais são? [Guia Completo]. **Legalcloud**, Análise de leis, LGPD, 4 nov. 2020. Disponível em: https://bit.ly/3siaVqV. Acesso em: 20 dez. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Presidência da República – Secretaria-Geral - Subchefia para Assuntos Jurídicos. Disponível em: https://bit.ly/2QBxU28. Acesso em: 25 out. 2020.

CARVALHO, T. *Sites* de bancos: perguntas e respostas sobre segurança. **TechTudo**, 8 out. 2018. Disponível em: https://glo.bo/2Qv5uGR. Acesso em: 20 dez. 2020.

CERT.br. Golpes na internet. **Cartilha de segurança para internet**. Disponível em: https://bit.ly/39aYpSh. Acesso em: 19 dez. 2020.

CONCEITOS. **Transação – Conceito, o que é, significado.** Disponível em: https://bit.ly/3lKBEK0. Acesso em: 19 dez. 2020.

MONITOR. **Monitor das fraudes.** Disponível em: http://www.fraudes.org. Acesso em: 20 dez. 2020.

OLIVEIRA, R. C. Q. **Tópicos de segurança da informação.** São Paulo: Editora Senac São Paulo, 2017.

REDE Nacional de Ensino e Pesquisa. **Catálogo de fraudes.** Disponível em: https://bit.ly/31bRUKz. Acesso em: 20 dez. 2020.