FOCO NO MERCADO DE TRABALHO

GESTÃO E POLÍTICAS DE SEGURANÇA

Emilio Tissato Nakamura

O QUE É SGSI?

O Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de políticas, processos e procedimentos, entre outros controles, para definir e prover segurança da informação em uma empresa.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você, como especialista em segurança e privacidade de uma plataforma digital, tem grandes responsabilidades. O planejamento dos principais aspectos que a empresa deve considerar para a segurança e privacidade é importante para direcionar a estratégia da empresa. O foco deste planejamento está na segurança em transações *web*, que complementa a segurança da informação da plataforma digital em si. Como a plataforma digital está em um provedor de nuvem, há vários aspectos como a arquitetura segura, desenvolvimento seguro, gestão de vulnerabilidades e gestão de continuidade de negócios, por exemplo.

Para a segurança em transações web, você pode começar o seu planejamento considerando os seguintes aspectos, os quais devem ser detalhados e desenvolvidos:

- Transação parte do usuário, que utiliza dispositivos e possui instalados aplicativos ou aplicações.
- Transação trafega pela internet, passando pelo provedor de internet.
- Transação chega à empresa e os dados são processados e armazenados.
- Há ameaças no ambiente do usuário, do provedor de internet e da empresa.
- Se o usuário for comprometido, a empresa também pode ser.
- O que pode ser feito para que o usuário não seja comprometido.
- O que deve ser feito pela empresa após receber os dados pessoais e transacionais.

O ponto central a ser planejado é que, além dos controles de segurança para proteger a transmissão dos dados dos clientes para a sua empresa, usando HTTPS/TLS/SSL, os clientes são parte central da segurança e privacidade, pois transações fraudulentas podem chegar à empresa a partir deles.

Mostre que pode haver o furto de identidade, a captura da senha, a captura da senha de transação, a modificação da transação e a interrupção do acesso. Essas ameaças existem no ambiente do cliente, no ambiente de internet e no próprio ambiente da empresa, que utiliza um provedor de nuvem.

Mostre que, no ambiente do cliente, os golpes na internet potencializam as ameaças, aumentando o nível de risco. E, como é o ambiente com menor controle, o desafio é maior nos clientes. Apresente os principais golpes na internet que podem comprometer a empresa, com destaque para o *phishing* e o *pharming*.

Defina a partir deste mapeamento um plano de conscientização para os clientes, minimizando as probabilidades deles caírem em fraudes na *internet*, e também de serem vítimas de *malwares*. Dentre as dicas, podem ser inclusos pontos como não clicar em *links* recebidos por e-mails e SMS, além de verificar sempre se uma conexão segura está estabelecida com a empresa, verificando os dados do certificado digital.

Um outro ponto importante para aumentar o nível de segurança é o uso de autenticação de duplo fator. Com este controle de segurança, em caso de furto de identidade, ainda é necessário o dispositivo móvel para o acesso aos serviços da empresa, o que torna o acesso indevido mais difícil.

Com relação à privacidade e proteção de dados pessoais, o planejamento deve incluir os avisos de privacidade na coleta das informações dos clientes. Além disso, a proteção destes dados pela empresa é parte da estratégia de segurança e privacidade, com o reforço de que há sanções previstas na LGPD.

Outro ponto importante a ser planejado são os processos e mecanismos para o atendimento às solicitações dos clientes, que podem consultar e solicitar a remoção dos seus dados pessoais.

Assim, com o tratamento destes principais aspectos, a empresa poderá operar com a necessária segurança e privacidade, minimizando os problemas de acessos a partir de clientes falsos, resultando em melhores resultados.

AVANÇANDO NA PRÁTICA

AUMENTANDO A SEGURANÇA NO ACESSO PELO NAVEGADOR

Os clientes de sua empresa virtual fazem o acesso pelo navegador, digitando o *link*. Você já implementou a segurança do servidor e envia constantemente mensagens para seus clientes para que eles aumentem o nível de conscientização e não caiam em golpes que podem levar ao furto de identidade, que no final resulta em prejuízos para a sua empresa. Cite os pontos que podem levar à contaminação do ambiente do cliente e por que evitar o furto de identidade é crucial para a sua empresa. Além disso, cite algumas possibilidades para você aumentar a segurança no acesso do cliente pelo navegador.

Ver anotações

RESOLUÇÃO

A empresa deve evitar as transações maliciosas, que podem chegar de duas formas principais: a partir de um criminoso que furtou a identidade do cliente e faz as transações como se fosse ele, utilizando recursos financeiros também de terceiros; e a partir de transações modificadas que partem do cliente legítimo, mas com os dados alterados para beneficiar o criminoso. A identidade pode ser furtada com a instalação de *malwares* que capturam os dados, os quais podem contaminar os clientes com o uso de *phishing* ou *pharming* como principal vetor, além de poder ser pela exploração de vulnerabilidades em diferentes componentes do dispositivo do cliente. Com o *phishing*, o cliente pode clicar em um *link* que leva para um site falso que coleta os dados de acesso e dados pessoais, incluindo o nome de usuário e senha. O *phishing* também pode fazer com que *malwares* sejam instalados quando executados pelos clientes. Os *malwares* podem também modificar os dados das transações na saída do ambiente do cliente e a empresa recebe essas transações adulteradas.

Uma vez com as credenciais do cliente, o agente de ameaça pode fazer as transações como se fosse ele, porém em benefício próprio.

Um mecanismo tradicional de se utilizar para evitar o uso de identidades furtadas é o uso de autenticação de dois passos ou de duplo fator. Em autenticação, os fatores são algo que o usuário sabe (como senhas), algo que o usuário possui (como *tokens* ou dispositivos móveis) ou algo que o usuário é (como a biometria). Com o uso de autenticação de duplo fator, é necessário, além da senha, um outro elemento, como um código único temporário enviado ao dispositivo móvel do usuário via SMS.

Há ainda a possibilidade de utilizar mecanismos de segurança que fazem uma proteção contra *malwares* para evitar a contaminação pelos usuários. Estes mecanismos devem ser instalados e fazem a proteção contra *malwares*, mas apresentam pontos negativos, como o uso de recursos computacionais dos dispositivos dos usuários, bem como a interferência na usabilidade.

Assim, como profissional de segurança, você deve adotar a abordagem em camadas, podendo utilizar ainda controles de segurança como processos de validação de transações ou uso de plataformas antifraude. Uma visão de riscos é fundamental, já que os controles de segurança podem afetar tanto a usabilidade dos clientes quanto a própria operação, que pode ficar mais complexa com as validações. Uma forma de flexibilizar as validações é a adoção de níveis, com base, por exemplo, em valores das transações. Deste modo, transações maiores teriam validações mais estruturadas, enquanto as menores teriam validações mais automatizadas, por exemplo. Isto deve ser definido com uma visão de riscos, e deve ser dinâmica, com atualizações constantes.