Observatório
Sistema Fiep

Guia de SEGURANÇA CIBERNÉTICA para pequenas empresas

PARTE I

Sistema Fiep

FIEP
SESI
SENAI
IEL

Apresentação

Segundo Relatório de Ameaças à Segurança na Internet[1], cerca de 76% dos ataques cibernéticos mundiais ocorrem em empresas com menos de 100 funcionários. A razão disso? Os cibercriminosos, ou seja, as pessoas que cometem crimes cibernéticos sabem que as redes de computadores de pequenas empresas tendem a ser alvos mais fáceis e repletos de informações sobre clientes e fornecedores. Para uma pequena empresa, no entanto, o custo de uma violação de dados pode ser devastador já que um ataque cibernético pode custar em média cerca de US$ 3,5 mil por funcionário, levando à falência 60% dos negócios atingidos (MORGAN, 2020).

Felizmente, a segurança cibernética não é uma tarefa difícil. Existem medidas simples que, se implementadas, podem evitar ou reduzir significativamente o impacto dos incidentes de segurança cibernética mais comuns. Tendo em vista tal desafio, o Sistema Federação das Indústrias do Estado do Paraná (Sistema Fiep), por meio do Observatório Sistema Fiep, lança este guia projetado especificamente para pequenas empresas. Considerando que, muitas vezes, proprietários e gestores não têm tempo para entender a complexidade da internet ou estabelecer respostas complicadas a riscos cibernéticos, o documento foi elaborado com linguagem clara, ações simples e orientação personalizada para pequenos empreendimentos. Com mais essa ação, o Sistema Fiep espera colaborar para a prosperidade econômica do Paraná tendo como pano de fundo a resiliência das pequenas indústrias estaduais.

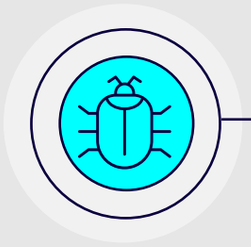
O Guia de Segurança Cibernética para Pequenas Empresas foi desmembrado em duas partes:

Parte I - Descreve os tipos de ameaças mais comuns e as estratégias para manter a segurança cibernética.

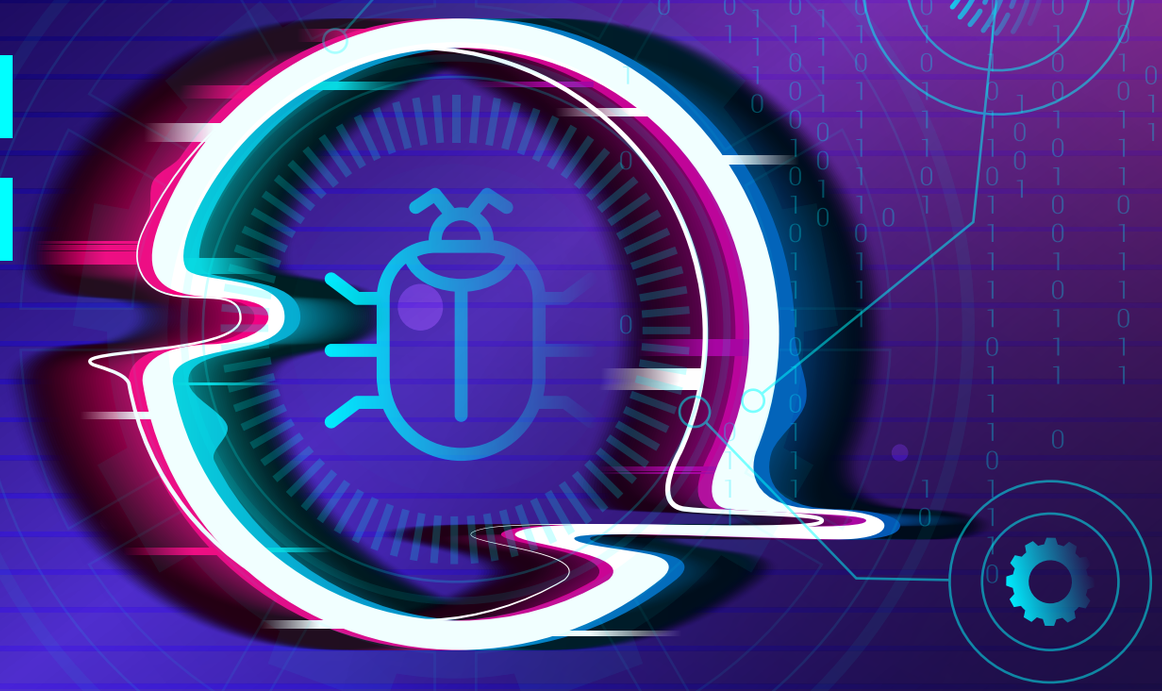
Parte II - Apresenta as ações para auxiliar na mitigação de incidentes de segurança cibernética causados por ameaças típicas.

[1]Elaborado pela Empresa Symantec, responsável pela linha de produtos Norton.

PARTE I



OS TIPOS DE AMEAÇAS CIBERNÉTICAS MAIS COMUNS



Para uma pequena empresa, mesmo o menor incidente cibernético pode ter impactos devastadores. Esta sessão identifica e explica os tipos mais comuns de ameaças cibernéticas e o que você pode fazer para proteger sua empresa.

Software malicioso (*malware*)

O que é?

***Software* não autorizado e projetado para causar danos. Podem incluir:**

Trojan: disfarça-se como *software* legítimo e cria "portas" na segurança para permitir a entrada de outro *malware.*

Spyware: espiona para obter acesso a informações como senhas, dados de cartão de crédito e hábitos de navegação.

Worm: infecta redes inteiras de dispositivos.

Botnets: redes de computadores infectados projetadas para funcionar sob o controle do invasor.

Por que se proteger?

O *malware* pode obter acesso a informações importantes, como números e senhas de bancos ou cartões de crédito. Também pode assumir o controle ou espionar o computador dos usuários. De posse de tais informações, os criminosos podem:

* Realizar roubos e furtos;
* Pregar peças ou pegadinhas;
* Praticar ativismo político-ideológico;
* Cometer atos de espionagem.

Quem ameaça?

Os criadores de *malware* podem estar em qualquer lugar do mundo. Eles só precisam de um computador, habilidades técnicas e más intenções. Os criminosos podem acessar facilmente ferramentas baratas para usar um *malware* contra sua empresa. **Não é pessoal — eles não estão direcionando os ataques especificamente contra você, são apenas negócios!**

Como se proteger?

Proteger-se de um *malware* conhecido é relativamente fácil. Sua empresa pode habilitar e configurar soluções antivírus e antimalware, incluindo *softwares* de *firewall* direcionados aos sistemas de informação e ativos. Como acontece com todo *software*, sua organização deve configurar essas soluções para atualizações e varreduras automáticas. Lembre-se sempre de:

- Habilitar soluções antimalware;
- Ativar os *firewalls* de *softwares*;
- Atualizar periodicamente seu sistema operacional;
- Modernizar *softwares* frequentemente;
- Fazer *backup* dos dados da sua empresa regularmente.

E-mails fraudulentos (*phishing*)

O que é?

E-mail **projetado para enganar destinatários.**

Por que se proteger?

O *phishing* são *e-mails* de "pesca" enviados por criminosos que utilizam nomes de indivíduos ou organizações conhecidos. Eles imitam frases, marcas e logotipos para parecerem reais, induzindo os usuários a clicarem em um *link* ou anexo. Tais *e-mails* enganam usuários, pedindo o fornecimento ou a confirmação de informações pessoais, como senhas e números de cartão de crédito, ou o pagamento de alguma conta falsa. Eles também podem enviar um anexo, projetado para parecer genuíno, com um *malware* anexado.

Quem ameaça?

Normalmente, os *e-mails* de *phishing* são enviados para milhares de pessoas. Mesmo que apenas uma pequena porcentagem dos destinatários caia no esquema, tais golpes podem obter dados e quantias de dinheiro significativas. Atualmente, existem três tipos de golpes mais comuns , listados a seguir.

Phishing: normalmente de baixa sofisticação, são *e-mails* gerais com sinais de alerta óbvios, enviados para milhares de alvos.

Spear phishing: corresponde a mensagens fraudulentas e sofisticadas enviadas a um indivíduo específico, geralmente proprietário da empresa, secretária ou gerente financeiro.

Whaling: *e-mails* de alta sofisticação, são *spear phishings* direcionados a peixes muito grandes, como CEOs.

Onde acontece?

Os golpes de *phishing* não se limitam a *e-mails.* Eles estão cada vez mais sofisticados, mais difíceis de serem detectados e podem alcançar SMS, mensagens instantâneas e mídias sociais.

Como se proteger?

Duvide e tenha cuidado com:

- Pedidos de dinheiro, especialmente urgentes;
- Mudanças de conta bancária;
- Abertura de anexos;
- Solicitações para verificar ou confirmar os detalhes de *login.*

Ransomware

O que é?

Software malicioso (*malware*) que bloqueia computadores e arquivos até que uma espécie de "resgate" seja pago. Os ataques de *ransomware* são normalmente realizados por meio de um *link* ou anexo de *e-mail*, mas com aparência legítima. Quando baixados ou abertos, a maioria dos *ransomwares* criptografa os arquivos do usuário e exige certa quantia em dinheiro para restaurar o acesso — normalmente pago com criptomoeda, como *Bitcoin*.

Por que se proteger?

Roubos com pedidos de resgate são crimes antigos e agora estão sendo cometidos de maneira *on-line*. O *ransomware* oferece aos cibercriminosos uma renda de baixo risco e alta recompensa, pois é extremamente fácil desenvolver e distribuir *softwares.* Também a favor dos cibercriminosos está o fato de que a maioria das pequenas empresas não está preparada para lidar com ataques de *ransomware*.

Onde acontece?

Os golpes de *ransomware* atingem pequenas, médias e grandes empresas. No entanto, como pequenas empresas costumam se preocupar menos com a segurança, elas se configuram como "porta" constante de ataques.

Como se proteger?

Lembre-se sempre de:

- Atualizar periodicamente seu sistema operacional;
- Modernizar *softwares* frequentemente;
- Fazer *backup* dos dados da sua empresa regularmente.

Hacking

O que é?

Hacking são as atividades que procuram comprometer dispositivos digitais, como computadores, *smartphones*, *tablets* e redes. Embora a prática nem sempre seja maliciosa, muitas atividades de *hacking* caracterizam-se como atividades ilegais na medida em que são motivadas por ganhos financeiros, protestos e coleta de informações (espionagem).

Como acontece?

Hacking ocorre quando os criminosos obtêm acesso não autorizado a computadores, *e-mails* ou sistemas, manipulando informações ou dados contidos. As técnicas comuns de *hacking* incorporam muitas das ameaças apresentadas, incluindo *botnets, ransomwares, trojans*, vírus e *worms.*

Como se proteger?

Para evitar que *hackers* entrem em seu sistema, lembre-se de:

- Usar senhas fortes;
- Utilizar autenticação de dois fatores;
- Escolher um provedor de serviços de internet que ofereça recursos de segurança integrados;
- Manter *softwares* de antivírus e antispyware atualizados;
- Instalar um *firewall* de rede;
- Criptografar dados e informações confidenciais.

AS ESTRATÉGIAS PARA MANTER A SEGURANÇA CIBERNÉTICA

Todo e qualquer tipo de empresa precisa estar ciente das ameaças e aplicar conscientemente medidas de segurança cibernética em todos os níveis. Considerando que normalmente as pequenas empresas carecem de recursos para uma equipe exclusiva de TI, esta seção apresenta as estratégias mais comuns adotadas por empresas mundo afora para aumentar a resiliência e a segurança de seus negócios.

Atualizações automáticas (*patch*)

O que é?

Versão nova, melhorada ou mais segura de um *software* (programa, aplicativo ou sistema operacional como Microsoft Windows ou Apple iOS) que sua empresa instalou em computadores ou dispositivos móveis. A atualização automática é um sistema padrão que atualiza seu *software* sempre que uma nova versão estiver disponível.

Por que realizar?

Atualização automática consiste em uma abordagem prática para manter os sistemas e aplicativos atualizados. Tal prática pode:

Melhorar a segurança *on-line*;

Proporcionar proteção em tempo real contra perda de dinheiro e dados;

Aprimorar recursos e eficiência de programas e aplicativos.

Quando executar?

As atualizações automáticas devem ser executadas todos os dias. Lembre-se de:

* Ativar ou confirmar as atualizações automáticas, especialmente para sistemas operacionais;
* Verificar regularmente se há atualizações disponíveis, especialmente para *software;*
* Instalar as atualizações o mais rápido possível (caso as atualizações automáticas não estejam disponíveis);
* Definir um horário conveniente para atualizações automáticas para evitar interrupções das atividades diárias da empresa;
* Ativar as atualizações automáticas do *software* antivírus.

Antivírus

O que é?

Programa de computador que detecta e exclui ameaças, evitando a instalação de aplicativos maliciosos e a contaminação de outros computadores e dispositivos conectados em sua rede. Existem dois tipos básicos de antivírus: domésticos e corporativos. Um erro comum que ocorre na maioria das pequenas e médias empresas é o uso de versões domésticas para a garantia da segurança.

Por que realizar?

Optar por um bom antivírus corporativo pode trazer uma série de benefícios para a sua empresa como:

* Rapidez na detecção de vírus e outros *malwares*;
* Gestão de processos simplificada;
* Avisos e atualizações automáticas;
* Prevenção de fraudes bancárias;
* Proteção de dados da empresa;
* Suporte técnico.

Quando executar?

Os antivírus têm ferramentas para a verificação períodica, que será executada automaticamente. A verificação monitora seu sistema e examina se foram introduzidos vírus por meio de anexos de *e-mail* ou ações do navegador, como ao clicar em *links* para *download.* Após a verificação, são criados relatórios com informações sobre o que foi encontrado e, se possível, são reparados os danos que o vírus possa ter causado. Um programa antivírus abrangente baixa e instala automaticamente as definições de vírus mais recentes antes de executar uma verificação, garantindo que a sua empresa esteja protegida contra todas as novas ameaças conhecidas. Essa proteção proativa reconhece comportamentos maliciosos que podem indicar uma tentativa de infectar seu computador, neutralizando-os logo no início.

Backup e criptografia

O que é?

Cópia digital das informações mais importantes de sua empresa, por exemplo, dados sobre clientes e vendas. Um *backup* automático é um tipo de sistema que faz a cópia de dados automaticamente, sem intervenção humana. Esse processo pode ser realizado por meio da criptografia, técnica de construção e análise de protocolos para comunicação segura na presença de terceiros, chamados "adversários".

Por que realizar?

Realizar *backups* automáticos e periódicos representa o meio mais rápido e fácil para colocar sua empresa de volta em funcionamento caso determinadas informações sejam perdidas, roubadas ou destruídas. *Backups* podem também proteger a credibilidade do seu negócio e ajudar a cumprir eventuais obrigações legais.

Quando executar?

Os *backups* automáticos devem ser executados todos os dias. Lembre-se de:

* Escolher um sistema de *backup* certo para sua empresa;
* Testar a restauração seu *backup* regularmente;
* Criptografar *backups*;
* Armazenar *backups* criptografados em um local externo seguro;
* Criar um *backup* físico em um local seguro fora da empresa;
* Desconectar e remover com segurança seu dispositivo de armazenamento de *backup* para garantir a proteção dos dados em caso de um incidente cibernético.

Autenticação de dois fatores (ou multifator)

O que é?

Medida de segurança que requer duas ou mais provas de identidade para conceder acesso ao usuário. A autenticação multifator normalmente requer uma combinação de algo que o usuário conhece (como PIN e pergunta secreta), possui fisicamente (como cartão e *token*) ou não (como impressão digital e retina).

Por que realizar?

As múltiplas camadas de provas de identidade tornam a vida muito mais difícil para criminosos atacarem sua empresa. Eles podem até conseguir roubar uma prova de identidade (como o PIN), mas ainda precisam obter e usar as outras (como a digital).

Quando executar?

As pequenas empresas devem implementar a autenticação multifator sempre que possível. Algumas opções podem incluir, mas não estão limitadas a:

- ***Token* físico;**
- **PIN aleatório;**
- ***Biometria* ou impressão digital;**
- **Aplicativo autenticador;**
- ***E-mail;***
- **SMS.**

Segurança de perímetro

O que é?

Linha de divisão imaginária que separa a rede e os dispositivos da sua empresa de outras redes e também da internet. Fazer segurança de perímetro significa controlar tudo que tenta ultrapassar essa barreira. Por exemplo, se uma pessoa que não faz parte da empresa tentar acessar a sua rede, a segurança de perímetro vai impedir que ela tenha sucesso.

Por que utilizar?

Se o perímetro não está protegido, os dados da empresa ficam vulneráveis e podem ser roubados e divulgados sem consentimento, arquivos podem ser acessados indevidamente e as ameaças têm caminho livre. Ao contrário, com uma boa segurança de perímetro, você conseguirá conter ataques de invasores e impedir acessos maliciosos.

Como executar?

Não existe um caminho certo para defesa de perímetro. Isso irá depender do porte e do tipo de negócios de sua empresa. No entanto, alguns exemplos e como implementar segurança de perímetro podem ser apontados.

Primeiramente, sua empresa deve usar um *firewall*, ou seja, um sistema de segurança de rede que monitora e controla o fluxo do tráfego por meio de um conjunto de regras de segurança. Os *firewalls* se posicionam nas entradas das redes, defendendo-se de ameaças cibernéticas. O tipo mais comum de *firewall* se chama Sistema de Nome de Domínio (DNS). Genericamente, o DNS é equivalente a uma lista telefônica que traduz nomes de domínio em endereços de protocolo de internet (IP). Os *firewalls* DNS podem impedir que usuários e dispositivos se conectem a *sites* mal-intencionados, já que se aproveita da inteligência de

ameaças disponibilizadas pela comunidade de segurança cibernética.

Existem riscos adicionais a serem considerados se a sua empresa permitir que os funcionários trabalhem fora do escritório e se conectem remotamente a uma rede a partir da internet. Se isso ocorrer, você deve compreender os benefícios e os riscos associados ao uso de uma conexão de rede privada virtual (VPN), garantindo a utilização de criptografia e autenticação de dois fatores.

Se sua empresa utiliza redes sem fio (Wi-Fi), evite conectar-se a redes públicas. Nesse caso, é recomendável a utilização de redes seguras e que forneçam autenticação de usuário forte (ou seja, use o protocolo de segurança sem fio WPA2). Se sua empresa oferece serviços públicos de Wi-Fi para visitantes e convidados, nunca conecte sua rede e seus recursos internos (impressoras, por exemplo) à rede pública.

Certifique-se de segmentar terminais de ponto de venda e sistemas financeiros, isolando-os da internet e de outras áreas da rede corporativa por meio de um *firewall*. Sua empresa deve seguir o Padrão de Segurança de Dados da Indústria de Cartão de Pagamento (PCI-DSS), que é um padrão de segurança de informações destinado a aumentar os controles sobre dados de cartões de crédito e reduzir fraudes.

Por fim, sua organização também deve ter medidas de segurança para proteger seus serviços de *e-mail*. Recomendamos que você implemente o DMARC, um sistema de autenticação de *e-mail* que pode detectar e impedir a falsificação do endereço do remetente. O DMARC também trata de *spam* e *e-mails* maliciosos.

Lembre-se de:

- Instalar um *firewall* direcionado à fronteira entre a rede corporativa e a *internet;*
- Implementar um *firewall* DNS para solicitações de saída para a *internet*;
- Usar a conectividade VPN segura com autenticação de dois fatores para todos os acessos remotos à rede corporativa;
- Usar Wi-Fi seguro para redes internas;
- Evitar conectar redes Wi-Fi publicamente acessíveis à sua rede corporativa;
- Seguir o PCI-DSS para todos os terminais de ponto de venda;
- Usar um *firewall* para isolar terminais de ponto de venda da internet e de outras áreas da rede corporativa;
- Implementar o DMARC para serviços de *e-mail*.

Controle de acesso

O que é?

Processo para regular os níveis de acesso a dados e sistemas dentro do ambiente de computação de uma empresa. O controle é uma forma de limitar o acesso a um ou mais sistemas computacionais. Ele permite que os proprietários de negócios:

Decidam quem terá privilégios de acesso;

Determinem quais funções exigem determinados tipos de permissões;

Apliquem limites de controle dentro da equipe.

Por que utilizar?

Para minimizar o risco de acesso não autorizado a informações importantes. Como muitas empresas empregam funcionários terceirizados ou contratam fornecedores (por exemplo, empresas de hospedagem de *sites*), os sistemas de controle de acesso podem ajudar a proteger o negócio, limitando o acesso a:

* Redes;
* Arquivos;
* Formulários;
* Dados sensíveis.

Como executar?

Dependendo da natureza do seu negócio, o “princípio do menor privilégio” é a abordagem mais segura para a maioria das empresas. Ele dá aos usuários somente as permissões mínimas para realização do trabalho. A utilização desse princípio pode reduzir o risco de um “interno” colocar acidentalmente o seu negócio em perigo. Lembre-se de:

Atribuir contas exclusivas para cada usuário;

Fornecer contas de usuário com o mínimo de privilégio;

Não compartilhar senhas;

Revogar contas de ex-colaboradores;

Implementar um sistema de autorização centralizado.

Política de senhas

O que é?

Incentivo ao uso de frases-senha para acessar um sistema, programa ou serviço.

As frases-senha são mais eficazes quando são:

- Usadas com autenticação multifator;
- Únicas e não reutilizáveis;
- Longas, com muitas palavras;
- Complexas, com caracteres maiúsculos, símbolos e pontuação;
- Fáceis de lembrar.

Por que utilizar?

As frases-senha são mais convenientes e difíceis de “quebrar” quando comparadas às senhas comuns. Além disso, são mais fáceis de lembrar do que caracteres aleatórios e, “naturalmente”, atendem a todos os requisitos exigidos para uma senha “forte” (ou seja, são montadas com letras maiúsculas, minúsculas, símbolos e pontuação).

Onde empregar?

As frases-senha devem ser utilizadas em todos os dispositivos fixos e móveis. As frases secretas aumentarão significativamente a segurança da sua empresa. Veja abaixo uma comparação entre senhas “comuns” e frases-senha.

Senha	Dificuldade de lembrança	Comentário
senha123	Muito fácil	Uma das senhas mais usadas no planeta.
Spaghetti95!	Fácil	Alguma complexidade, mas a extensão é muito curta. Fácil de lembrar e “quebrar”.
5 macarrão! 95	Um pouco fácil	Possui um nível de complexidade maior em relação à senha anterior, mas a extensão ainda é muito curta. Também é fácil de lembrar e “quebrar”.
A & d8J + 1!	Muito difícil	Moderadamente complexo e mais curta do que as senhas Anteriores. Difícil de lembrar e fácil de “quebrar”.
Eu não gosto de abacaxi na minha pizza!	Fácil	Excelente extensão, pois contêm 35 caracteres. A complexidade é naturalmente alta devido ao uso de ponto de exclamação e espaços. Muito fácil de lembrar e extremamente difícil de decifrar.

Como implementar?

Sua empresa deve implementar uma política de senha que descreva os requisitos (por exemplo, quando uma senha deve ser alterada). Também pode ser considerado o uso de gerenciadores de senhas para ajudar a administrar várias senhas ou gerar senhas complexas. Lembre-se de:

* Implementar uma política de senha;
* Usar frases de acesso para senhas;
* Implementar autenticação de dois fatores sempre que possível.

Plano de resposta

O que é?

Plano elaborado para garantir a detecção, a resposta e a recuperação diante de um incidente ou ataque cibernético.

Por que realizar?

Um plano eficaz limita as interrupções de serviços internos, atendimento a clientes e parceiros, reduzindo a perda de dados e os danos à reputação da empresa.

Como executar?

Um plano de resposta “escrito” garante parcialmente que colaboradores e interessados estejam aptos a realizar as tarefas necessárias para lidar com um incidente. Lembre-se de:

- Especificar as funções e responsabilidades dos envolvidos na resposta;
- Fornecer informações de contato para todos os envolvidos nas atividades de resposta;
- Fornecer instruções detalhadas sobre como lidar com incidentes comuns;
- Especificar ações necessárias para a elaboração de relatórios obrigatórios.

Devido à falta de monitoramento, muitos incidentes cibernéticos passam despercebidos por um longo tempo, resultando em recuperações mais complicadas e caras. Sua empresa deve considerar a implementação de uma solução para detectar, monitorar e responder os incidentes, como um sistema de gerenciamento de informações e eventos de segurança. Além da cobertura de responsabilidade, sua empresa também deve considerar a compra de uma apólice de seguro de segurança cibernética que cubra as atividades de resposta e recuperação a incidentes.

Treinamento

O que é?

Formação profissional ou ensino de habilidades práticas para proteger sua equipe e seus negócios contra ameaças cibernéticas. O treinamento consiste em um plano de resposta a incidentes de segurança cibernética que pode ajudar a mudar os hábitos e comportamentos de funcionários, criando senso de responsabilidade compartilhada para manter a segurança da empresa. Seu plano de resposta a incidentes de segurança cibernética ensina a equipe a:

- Reconhecer;
- Evitar;
- Reportar;
- Retirar;
- Recuperar.

Por que realizar?

Um programa de treinamento de segurança digital é vital já que funcionários representam a melhor linha de defesa contra ameaças cibernéticas. Sabendo que funcionários podem cometer erros, é imperativo que as informações da sua empresa sejam protegidas.

Quando implementar?

Conscientização e treinamento sobre segurança cibernética devem se constituir como uma ação contínua e regular dentro de qualquer empresa. Como as ameaças estão cada vez mais constantes e diárias, manter todos atualizados pode ser a diferença. Lembre-se de:

* Ofertar, atualizar e repetir treinamentos regularmente;
* Criar um plano de resposta a incidentes cibernéticos;
* Recompensar os funcionários que encontrarem ameaças;
* Criar e incentivar uma cultura de segurança cibernética.

Glossário

ANTIMALWARE – programa de *software* desenvolvido para detectar e eliminar *malwares.*

ANTIVÍRUS – programa de *software* desenvolvido para proteger seu computador ou rede contra vírus de computador.

APLICATIVO – também conhecido como *app*, corresponde a um *software* comumente usado em *smartphones* ou *tablets.*

APLICATIVO AUTENTICADOR – aplicativo usado para confirmar a identidade e permitir o acesso de determinados usuários.

BIOMETRIA – identificação de uma pessoa por meio da medição de suas características biológicas, como impressão digital ou voz.

***BITCOIN* –** moeda digital (criptomoeda), usada na internet para compra e venda vários serviços.

***BOTNETS* –** rede de computadores que foi infectada por *softwares* maliciosos e pode ser controlada remotamente.

CIBERCRIMINOSO - qualquer indivíduo que hackeou, ou seja, burlou ilegalmente um sistema de computador para danificar ou roubar informações.

CONFIGURAÇÕES-PADRÃO - estrutura que um computador, sistema operacional ou programa predeterminou para o usuário.

CRIPTOGRAFIA - processo de tornar os dados ilegíveis por terceiros com a finalidade de impedir que tenham acesso ao seu conteúdo.

DADOS - são informações que incluem arquivos, textos, números, imagens, sons ou vídeos.

DMARC (*DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE*) – padrão técnico criado para reduzir as fraudes e os abusos via *e-mail*, validando as mensagens enviadas e padronizando o modo com que provedores fazem a leitura e a autenticação dos *e-mails* recebidos.

***ENDPOINT* –** utilizado para definir pontos de comunicação de acesso a uma aplicação (*endpoints* de comunicação) ou como parte de uma estrutura de segurança de rede (segurança de rede).

***FIREWALL* –** dispositivo de uma rede de computadores, na forma de um programa ou equipamento físico, que tem por objetivo aplicar uma política de segurança a determinado ponto da rede.

***GATEWAY* –** espécie de "fio condutor" da conexão do dispositivo com a internet que age com o objetivo de obter as informações requeridas previamente pelo usuário.

***HOST* –** qualquer máquina ou computador conectado a uma rede que oferece informações, recursos, serviços e aplicações a usuários ou outros nós na rede.

NUVEM - rede de servidores remotos que fornecem poder de processamento e armazenamento massivo e distribuído.

***PATCH* –** programa de computador criado para atualizar ou corrigir um *software* de forma a melhorar sua usabilidade ou *performance.*

PCI-DSS (PADRÃO DE SEGURANÇA DE DADOS DA INDÚSTRIA DE CARTÃO DE PAGAMENTO) – padrão de segurança de informações para organizações que lidam com cartões de crédito.

***PHISHING* –** técnica de engenharia social usada para enganar usuários e obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito.

PIN – nome usual para as senhas de pelo menos quatro caracteres usadas em *chips* de telefonia celular, cartões de tecnologia *smart card* e outras aplicações.

RDP (*REMOTE DESKTOP PROTOCOL*) – protocolo multicanal que permite que um usuário se conecte a um computador rodando o *Microsoft Terminal Services.*

REDE - coleção de computadores, servidores, *mainframes*, dispositivos de rede, periféricos ou outros dispositivos conectados uns aos outros para permitir o compartilhamento de dados.

***SANDBOX* –** mecanismo de segurança que separa programas em execução, normalmente utilizado para mitigar falhas do sistema e/ou vulnerabilidades de algum *software.*

SISTEMA DE NOME DE DOMÍNIO (DNS) – sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à internet.

SISTEMA OPERACIONAL - *software* instalado no disco rígido de um computador que permite ao *hardware* se comunicar e executar programas.

SMS (*SHORT MESSAGE SERVICE*) – serviço disponível em celulares que permite o envio de mensagens curtas.

***SOFTWARE* -** comumente conhecido como programas, diz respeito ao conjunto de instruções que permitem ao usuário interagir com um computador, *hardware* ou executar tarefas.

***SPEAR PHISHING* –** técnica de engenharia social usada para enganar usuários e obter informações confidenciais.

SPF (*SENDER POLICY FRAMEWORK*) – sistema que evita que outros domínios enviem *e-mails* não autorizados.

***SPYWARE* -** programa projetado para coletar secretamente informações sobre a atividade de um usuário. Geralmente é instalado sem o conhecimento do usuário quando ele clica em um *link.*

SSH (*SECURE SHELL*) – protocolo de rede criptográfico para operação de serviços de rede que atuam sobre uma rede insegura.

***TOKEN* -** dispositivo físico, normalmente em formato de chaveiro, que gera um código de segurança para uso em redes ou aplicativos.

***TROJAN* -** tipo de *malware* geralmente disfarçado de *software* legítimo, usado por criminosos cibernéticos para obter acesso aos sistemas dos usuários.

VÍRUS - programa projetado para causar danos, roubar informações pessoais, modificar dados, enviar *e-mail*, exibir mensagens ou a combinação dessas ações.

VPN (*VIRTUAL PRIVATE NETWORK*) – rede de comunicações privada construída sobre uma rede de comunicações pública.

***WHALING* –** técnica de engenharia social usada para enganar usuários e obter informações confidenciais.

***WORM* –** programa independente, do tipo *malware*, que se autorreplica com o objetivo de se espalhar para outros computadores.

Referências

AUSTRÁLIA. Australian Cyber Security Centre. **Small bussiness cyber security guide**. Disponível em: <https://cyber.gc.ca/en/guidance/cyber-security-small-business>. Acesso em: 6 abr. 2021.

AUSTRÁLIA. Australian Cyber Security Centre. **Cyber security: the small business best practice guide**. Disponível em: <https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-research-report.pdf>. Acesso em: 6 abr. 2021.

ESTADOS UNIDOS. **Cybersecurity for small business**. Disponível em: <https://www.fcc.gov/general/cybersecurity-small-business>. Acesso em: 6 abr. 2021.

ESTADOS UNIDOS. **Stay safe from cybersecurity threats**. Disponível em: <https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats>. Acesso em: 6 abr. 2021.

ESTADOS UNIDOS. **Small business cybersecurity corner**. Disponível em: <https://www.nist.gov/itl/smallbusinesscyber>. Acesso em: 6 abr. 2021.

MORGAN, S. **Cybercrime to cost the world $10.5 trillion annually By 2025**. Cybercrime Magazine. Disponível em: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>. Acesso em: 06 abr. 2021.

REINO UNIDO. **Small business guide:** cyber security. Disponível em: <https://www.ncsc.gov.uk/collection/small-business-guide>. Acesso em: 6 abr. 2021.

THE UK DOMAIN. **Cyber security for SMEs**. Disponível em: <https://www.theukdomain.uk/get-online/cyber-security-for-smes/>. Acesso em: 6 abr. 2021.

REALIZAÇÃO

Sistema Federação das Indústrias do Estado do Paraná – Sistema Fiep

Presidente
Carlos Valter Martins Pedro

Serviço Social da Indústria – Departamento Regional do Paraná

Serviço Nacional de Aprendizagem Industrial – Departamento Regional do Paraná

Superintendente do Sesi/PR e Diretor Regional do Senai/PR
José Antonio Fares

Observatório Sistema Fiep
Coordenação Executiva
Marilia de Souza

Coordenação Técnica
Raquel Valença

Autoria
Michelli Gonçalves Stumm

Projeto Gráfico e Diagramação
Katia Villagra

Revisão de Texto
Camila Rigon Peixoto