Métodos mais utilizados no vazamento de dados nas organizações e meios de prevenção

Izaias Maia Vieira, Fatec Americana - Ministro Ralph Biasi
izaias.vieira@fatec.sp.gov.br
Matheus Wilson Ramos Pereira, Fatec Americana - Ministro Ralph Biasi
matheus.pereira42@fatec.sp.gov.br
Daives Arakem Bergamasco, Fatec Americana - Ministro Ralph Biasi
daives.bergamasco@fatec.sp.gov.br

Resumo

Este trabalho aborda a dificuldade em manter os dados seguros nas organizações, os crescentes e mais comuns ataques e invasões com o objetivo de se apropriar de dados de terceiros, procurando lucrar com a comercialização ou exposição desses dados. O objetivo deste trabalho é apresentar os fatores mais comuns onde ocorrem os vazamentos, exposição e roubos de dados. Por meio dessa pesquisa serão abordadas as três principais formas mais utilizadas por criminosos virtuais na atualidade, sendo a mais frágil e ao mesmo tempo a mais importante: o fator humano, seguido por ataques phishing e ransomware. Diante disso é evidente a importância de treinamentos e conscientização dos colaboradores, bem como a utilização correta dos sistemas e dispositivos, a adoção de boas práticas de segurança da informação, monitoramento estratégico no uso da infraestrutura e a definição de um plano de continuidade dos negócios, de forma a melhorar a segurança dos dados. Conclui-se que as melhores práticas alinhadas com treinamento e conscientização juntamente com métodos de prevenção, e a utilização corretas dos dispositivos de infraestrutura, aprimoram a segurança dos dados gerenciados e minimizam as chances de ataques bem-sucedidos.
Palavras-chave: Informação. Dados. Segurança. Phishing. Ransomware.

Abstract

This work addresses the difficulty in keeping data safe in organizations, the growing and more common attacks and invasions with the objective of appropriating third-party data, seeking to profit from the commercialization or exposure of this data. The objective of this work is to present the most common factors where data leaks, exposure and theft occur. Through this research, the three main forms most used by cyber criminals today will be the same addressed, the most fragile and at the time the most important: the human factor, followed by phishing and ransomware attacks. In view of this, the importance of training and awareness of employees is evident, as well as the correct use of systems and devices, the adoption of good information security practices, strategic monitoring of the use of infrastructure and the definition of a business continuity plan, in order to improve data security. It is concluded that best practices aligned with training and awareness together with prevention methods, and the correct use of infrastructure devices, improve the security of managed data and minimize the chances of successful attacks.
Keywords*: Information. Data. Security. Phishing. Ransomware.*

1 Introdução

Quem não se preocupa com a segurança dos seus dados e informações? Sejam dados pessoais ou organizacionais devem estar bem protegidos, afinal, se esses dados caírem em mãos erradas eles podem ser utilizados de forma ilícita.

Frequentemente as organizações vem sendo alvos de ataques virtuais, ocorrendo o comprometimento de dados, exposição pública de informações confidenciais e interrupções de serviços. Como é possível proteger os dados e informações e qual a melhor forma de fazer isso?

A Tecnologia da Informação está presente em todos os setores. As organizações usam meios tecnológicos para utilizar, transmitir e receber os dados e informações, nesse contexto é necessário que ocorra a proteção desses dados em todas as fases de utilização.

Nos últimos anos, houve um grande aumento de vazamento de dados e roubo de informações, cada vez mais pessoas mal-intencionadas tem realizado esses tipos de ações, visando obter dados através de ataques cibernéticos com a intenção de usar ou repassar para quadrilhas especializadas em operações fraudulentas, prejudicando os proprietários das informações. Em outros casos *hackers* criptografam informações de empresas e negociam o resgate dessas informações através de pagamentos em dinheiro ou moedas digitais. Diante disso existe a Segurança da Informação que possui diretrizes e normas para a proteção das informações, a seguir veremos como ela pode ajudar a proteger dados e informações nas organizações.

Para auxiliar no tratamento das informações, existem no mercado diversas ferramentas, normas, manuais, tecnologias e mais recentemente, leis que tratam exclusivamente dos dados e que auxiliam no controle do tratamento dos dados.

Diante do exposto, foi proposto analisar neste artigo as falhas e ataques mais comuns existentes na atualidade e citar práticas e meios para que se possa garantir uma proteção eficaz no uso dos dados, seja na vida pessoal ou empresarial.

2 Referencial teórico

2.1 O que é informação?

A informação é um ou mais dados interpretados que agregam valores, sempre esteve presente no dia a dia das organizações e é de grande relevância nas tomadas de decisões.

Segundo Sêmola (2013), a informação é o ativo cada vez mais valorizado, que esteve sempre presente e cumpre um papel importante para a gestão do negócio e todos decidem suas ações e seus planos com base nas informações.

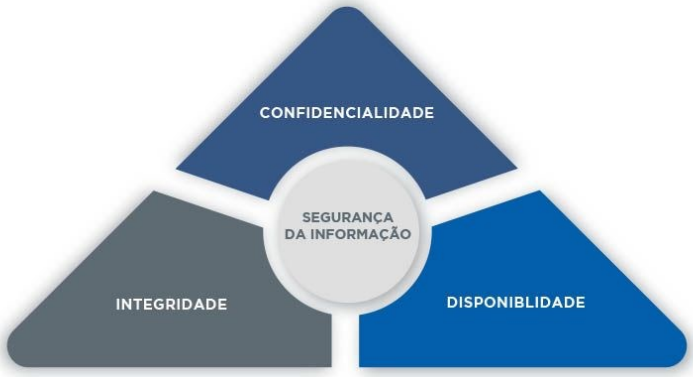
De acordo com Silva e Stein (2007), na sociedade atual a informação está disseminada em todos os seus setores e, cada vez mais, vem sendo vista como um recurso para empresas e pessoas que desejam alcançar resultados em sua vida pessoal, acadêmica, profissional ou social. Muitas dessas informações podem ser acessadas de forma aberta, sem custos e sem limitações, porém existem dados que precisam ser resguardados e protegidos, em função dos riscos que acarretariam seu amplo acesso por outros indivíduos ou empresas.

2.2 Segurança da informação

De acordo com Sêmola (2013), a Segurança da Informação pode ser definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua responsabilidade. De forma mais ampla, podemos

também considerá-la como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três conceitos do modelo clássico de segurança: confidencialidade, integridade e disponibilidade da informação como mosta a Figura 1.

Figura 1 - Pilares da Segurança da Informação



Fonte: https://blog.starti.com.br/mecanismos-da-seguranca

A confidencialidade tem a ver com a privacidade dos dados nas organizações, só devem ser acessadas por aqueles que tenham autorização, está relacionado as ações tomadas para garantir que as informações da empresa não sejam expostas de maneira indevida ou roubadas através de ciberataque ou outros tipos de invasões não autorizadas.

A integridade diz respeito às informações estarem precisas e confiáveis, de modo a validar que nenhum agente externo ou interno possa interferir, vindo a comprometer ou danificar esses dados tornando-os duvidosos.

A disponibilidade está relacionada ao acesso desses dados, a forma que os colaboradores, diretores e outros relacionados possam acessar essas informações.

A facilidade de transmitir dados e informações evoluiu, porém cresceu também de forma assustadora os acessos indevidos, sequestro de dados, invasões e roubos. Com tudo isso a Segurança da Informação se torna cada vez mais necessária e é um assunto que tomou conta do cotidiano das organizações que prezam pela segurança de suas informações.

De acordo com a NBR ISO/IEC 27002:2013, a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware.

2.3 Engenharia social

Engenharia social é uma técnica empregada por criminosos virtuais para enganar usuários a enviar dados confidenciais, os *hackers* podem tentar explorar a falta de conhecimento do usuário para infectar seus computadores com *malware* ou abrir *links* para sites infectados, geralmente esses métodos são simples e não levantam muitas suspeitas. Graças à velocidade da tecnologia, muitos clientes e funcionários não percebem o verdadeiro valor dos dados pessoais e não sabem exatamente como proteger essas informações.

De acordo com Mitnick e Simon (2003) os engenheiros sociais são indivíduos com a capacidade de manipular a confiança de outra pessoa de modo a obter acesso às informações

privadas. A disjunção dos termos “engenharia social” nos leva a um conceito literal, no qual, o termo “engenharia” aparece no sentido de construção e “social” por envolver pessoas.

De acordo com a *Kaspersky*[1], quase todo tipo de ataque contém algum método de engenharia social. O conhecido e-mail de *phishing*, onde tentam convencer os usuários de que são, de fato, de fontes legítimas, na esperança de conseguir obter qualquer dado pessoal ou corporativos. Os e-mails que contêm anexos cheios de vírus, por sua vez, muitas vezes alegam ser de contatos confiáveis ou oferecem conteúdo de mídia que parece inofensivo.

Em outros casos, os *hackers* usam métodos mais simples de engenharia social para conseguir acessar a rede ou o computador, como frequentar a praça de alimentação lugares públicos e bisbilhotar os usuários que trabalham com *tablets* ou *laptops*. Assim, se obtém muitos senhas e nomes de usuários, sem enviar sequer um e-mail ou escrever uma linha de código de vírus.

Alguns casos de engenharia social podem envolver até mesmo comunicação direta entre o invasor e a possível vítima, com a construção de uma relação entre os dois enquanto na verdade o invasor só quer roubar dados. Casos até mesmo de pessoas fingindo estar apaixonadas por uma vítima podem ocorrer, onde a vulnerabilidade causada pelo período das emoções à flor da pele acaba fazendo com que a pessoa vaze informações sensíveis para a outra.

De acordo com Mitnick e Simon (2003), a maioria das pessoas supõe que não será enganada, com base na crença de que a probabilidade de ser enganada é muito baixa; o atacante, entendendo isso como uma crença comum, faz a sua solicitação ser tão razoável que não levanta suspeita enquanto explora a confiança da vítima.

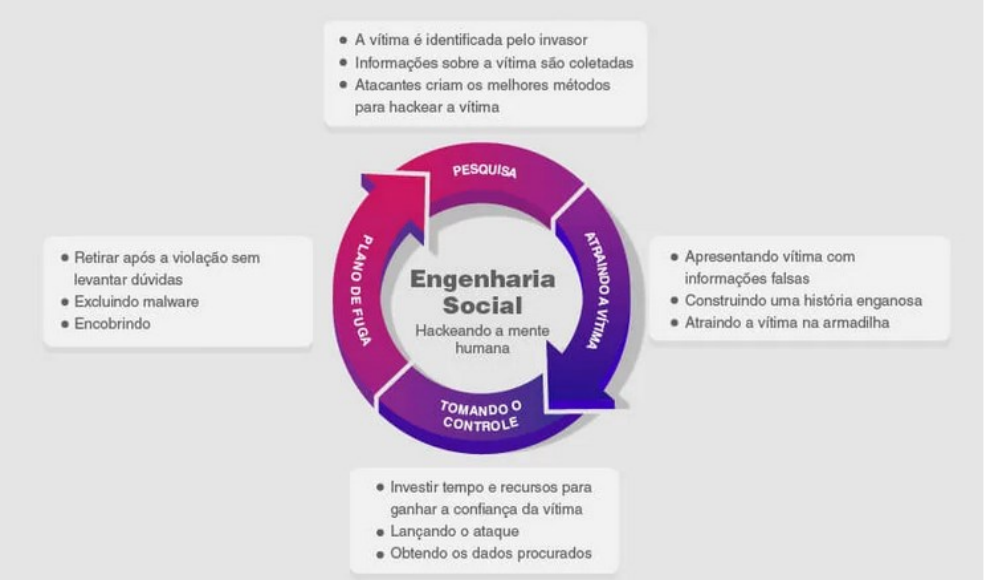
Dentre as ameaças que utilizam a engenharia social podemos destacar:

- Ataques de *Worms*: programa contendo código malicioso que ataca um computador e se espalha pela rede onde o criminoso virtual tenta atrair a atenção do usuário para o *link* ou arquivo infectado para que o usuário clique nele.
- Canais de envio de *links* com malware: os links para sites infectados podem ser enviados por e-mail, outros sistemas de mensagens instantâneas, ou até em salas de bate-papo na Internet. Frequentemente, os vírus de dispositivos móveis são enviados por mensagens SMS.
- Ataques de rede ponto a ponto (P2P): essas redes também são usadas para distribuir *malware*. Um *worm* ou cavalo de Troia aparece na rede P2P, mas recebe um nome que chama atenção e leva os usuários a baixar e abrir o arquivo.

A Figura 2 mostra de forma simplificada o processo que um engenheiro social utiliza para manipular suas vítimas e convencê-las a realizar aquilo que ele deseja:

Figura 2 - Ciclo de um ataque de engenharia social

[1] *Kaspersky* é uma das maiores empresas de cibersegurança no setor privado mundial com mais de 24 anos de experiência na indústria de cibersegurança.



Fonte: https://pt.safetydetectives.com/blog/o-que-e-engenharia-social-e-por-que-e-uma-ameaca-tao-grande/

É difícil se defender da engenharia social, já que essas fraudes são feitas para explorar impulsos e erros humanos, que não são tão simples de arrumar quanto uma atualização de *software* ou substituição de um *hardware*. Porém, existem várias meios que podem ajudar a identificar e se prevenir de tentativas de golpe. Na maioria das vezes são procedimentos para checar a veracidade das informações recebidas, um processo necessário e importante.

3 Vazamento de dados

3.1 Fator humano

Investir em ferramentas de Tecnologia da Informação, em sistemas específicos de segurança com alto grau de confiabilidade tem se tornado uma estratégia eficaz e importante para evitar incidentes de segurança da informação nas organizações, mas os fatos têm mostrado que esse não é o principal pilar na prevenção de ataques cibernéticos ou danos acidentais, o fator mais frágil desses pilares não está nos componentes eletrônicos ou sistemas de qualquer natureza, o fator humano desempenha um papel crucial e está ligado a maior parte dos incidentes por ciberataques, tornando-se dessa forma o elo mais fraco dessa cadeia, e tem um papel extremamente importante a desempenhar para ajudar a proteger a organização, ou seja, os colaboradores em todos os níveis são o elo mais importante que sustenta a engrenagem da segurança da informação.

De acordo com Beal (2003), pode-se afirmar que, considerando todos os aspectos envolvidos na criação e manutenção da segurança da informação num determinado ambiente, o fator humano é o elo mais frágil e provavelmente o mais complexo de ser tratado. Isso pode ser entendido facilmente quando se imagina que qualquer esquema de segurança pode ser derrubado, por exemplo, se o administrador de uma rede simplesmente divulgar sua senha para outra pessoa ela pode utilizar-se dos privilégios.

Quando os usuários não têm conhecimento suficiente sobre os perigos, ao abrirem *links* ou arquivos duvidosos ou que não conhecem a procedência, podem abrir portas de entrada para o invasor infectar o computador com algum tipo de vírus. Essas ações podem ser por negligência, má fé, imperícia ou falta de treinamento, criando assim meios para que ataques sejam bem-sucedidos.

3.2 Phishing

O *Phishing* é o crime de enganar as pessoas para que compartilhem informações confidenciais. São ataques de engenharia social e podem ter uma grande variedade de alvos ou pode ser um ataque direcionado focado em um indivíduo específico, dependendo do invasor. As vítimas acabam recebendo na maioria das vezes um e-mail ou uma mensagem de texto se passando por uma pessoa ou organização em que confiam, como um colega de trabalho, um banco ou um órgão governamental. O invasor geralmente adapta um e-mail para falar diretamente com você e inclui informações que apenas um conhecido saberia. Um invasor geralmente obtém essas informações após obter acesso aos seus dados pessoais. Os tipos de ataques de *phishing* variam de esquemas clássicos de *phishing* de e-mail a abordagens mais criativas, como *spear phishing* e *smishing*. Todos têm o mesmo propósito: roubar dados.

Se o e-mail for desse tipo, será muito difícil, mesmo para o destinatário mais cauteloso, não se tornar uma vítima, e se os usuários mordem a isca e clicam no *link*, eles enviam uma imitação de um *website* legítimo. A partir daí, eles pedem para fazer o *login* com nome de usuário e senha. Assim as informações de acesso são enviadas aos atacantes que as usam para realizar atos ilícitos ou extorquir mediante algum tipo de ameaça.

De acordo com a *Kaspersky*, um em cada cinco brasileiros sofreu pelo menos um ataque de *phishing* em 2020. Essa estatística coloca o Brasil como líder mundial em golpes dessa categoria, à frente de Portugal, França, Tunísia e Guiana Francesa, que completam a lista dos cinco países com maior índice de usuários alvo. Esses ataques se intensificaram com o início da pandemia do Covid-19, as ameaças contra dispositivos móveis cresceram mais de 120%. O levantamento mostra ainda que o índice de brasileiros alvos de *phishing* (20%) está acima da média mundial (13%).

O *phishing* não requer um conhecimento técnico muito sofisticado, na verdade, é o tipo mais simples, ao mesmo tempo, muito perigoso e eficiente porque ele ataca o computador mais vulnerável e poderoso do planeta: a mente humana. Nenhum sistema operacional está completamente seguro contra *phishing*, não importa quão eficiente é a segurança.

Apesar das inúmeras variedades de tipos de ataques de *phishing*, o denominador comum de todos os ataques de *phishing* é o uso de um falso pretexto para adquirir valores. De acordo com a *Trend Micro*[2], algumas das principais categorias incluem:

- ***Spear phishing:*** Tem como alvo um grupo específico ou tipo de indivíduo, como administradores de sistema de uma empresa. Por exemplo, um invasor pode executar um *spear phishing* com um funcionário cujas responsabilidades incluam autorizar pagamentos. O e-mail parece que foi enviado por um executivo da organização, solicitando que o funcionário faça o pagamento de uma quantia significativa para ele ou para um fornecedor, mas na verdade, o *link* de pagamento malicioso envia para o invasor.
- ***Whaling****:* É um tipo de phishing ainda mais direcionado, esses ataques geralmente têm como alvo um CEO, CFO ou qualquer CXX dentro de um setor ou negócio específico. Um e-mail de *whaling* pode indicar que a empresa está enfrentando consequências legais e que você precisa clicar no *link* para obter mais informações. O *link* leva você a uma página na qual é solicitado que você insira dados essenciais sobre a empresa, como ID fiscal e números de contas bancárias.

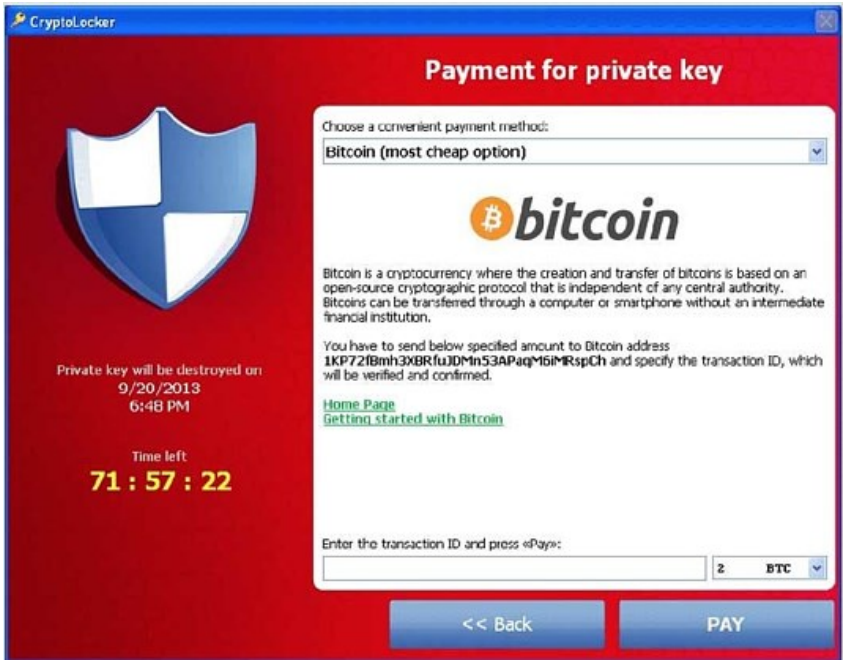
[2] *Trend Micro* é uma empresa multinacional de cibersegurança que atua no desenvolvimento de software de segurança.

- ***Smishing***: É um ataque que usa mensagens de texto ou serviço de mensagens curtas (SMS) para executar o ataque. Uma técnica comum de *smishing* é enviar uma mensagem a um telefone celular por meio de SMS que contém um *link* clicável ou um número de telefone de retorno. Um exemplo comum de ataque de *smishing* é uma mensagem SMS que parece ter vindo da sua instituição bancária. Ele informa que sua conta foi comprometida e que você precisa responder imediatamente. O invasor pede para você verificar o número da sua conta bancária. Depois que o invasor recebe as informações, o invasor tem o controle de sua conta bancária.
- ***Vishing****:* Este ataque é realizado por meio de uma chamada de voz. Daí o "v" em vez do "ph" no nome. Um ataque comum de *vishing* inclui uma ligação de alguém que afirma ser, por exemplo, um representante da Microsoft. Esta pessoa informa que detectou um vírus no seu computador. Em seguida, você será solicitado a fornecer os detalhes do cartão de crédito para que o invasor possa instalar uma versão atualizada do *software* antivírus em seu computador. O invasor agora tem as informações do seu cartão de crédito e provavelmente você instalou *malware* no seu computador.
- ***Phishing* de e-mail**: É o tipo mais comum de *phishing* e está em uso desde a década de 1990. Os criminosos enviam esses e-mails para todo e qualquer endereço de e-mail que possam obter. O e-mail geralmente informa que houve um comprometimento de sua conta e que você precisa responder imediatamente clicando em um *link* fornecido. Esses ataques são geralmente fáceis de detectar, pois o idioma do e-mail geralmente contém erros ortográficos e/ou gramaticais. Alguns e-mails são difíceis de reconhecer como ataques de *phishing*, especialmente quando a linguagem e a gramática são elaboradas com mais cuidado. Verificar a fonte do e-mail, o *link* para o qual você está sendo direcionado e se há uma linguagem suspeita podem fornecer pistas sobre a legitimidade da fonte.

3.3 Ransomware

O *ransomware* é um tipo de *malware* que criptografa arquivos, computadores e dispositivos móveis, podendo infectar um ou mais dispositivos da rede de uma empresa e impede os usuários de acessarem arquivos ou sistemas. Existem diversas formas de ataque desse *malware*, os atacantes podem enviar mensagens falsas se passando por autoridades legais informando que foi encontrado conteúdo ilícito no dispositivo, aplicativos não licenciados que o usuário utiliza, pedindo ao usuário que faça um pagamento para regularizar, ao clicar no botão, o *malware* é instalado; em outros casos, ao navegar pela internet os usuários visualizam *pop-up* com mensagem que o computador está infectado ou o navegador desatualizado, após o clique do usuário para supostamente resolver o problema o *malware* é instalado. Após o *malware* criptografar os arquivos, uma mensagem de resgate é exibida na tela com informações sobre pagamento, geralmente em criptomoedas, para receber a chave ou os arquivos descriptografados, instruções para transferência do valor e o prazo para o pagamento, como mostra a Figura 3.

Figura 3 - Mensagem de resgate de um ataque de *ransomware*



Fonte: https://www.avast.com/pt-br/c-how-to-remove-ransomware-pc/

De acordo com o relatório da *SonicWall* de Ameaças Cibernéticas 2021, foram registrados em torno de 623 milhões de tentativas de ataques globalmente, sendo 33 milhões de tentativas no Brasil somente em 2021, ocupando a 4ª posição, atrás apenas dos EUA, Alemanha e Reino Unido. Os pesquisadores do *SonicWall Capture Labs* rastrearam o aumento meteórico de *ransomware*, chegando a um recorde de 318,6 milhões a mais de ataques do que em 2020. Isso significa um aumento de 105%. O volume cresceu 232% desde 2019.

Os primeiros *malwares* desse tipo foram desenvolvidos no final da década de 1980. Já o primeiro *malware* moderno surgiu em 2005, em 2015, mais de 58% dos computadores corporativos foram atacados por *malware*, e os ataques de *cryptolocker* dobraram, segundo dados da *Kaspersky*. Enquanto o dispositivo estiver infectado com o *ransomware*, qualquer tentativa de abrir ou descriptografar os arquivos serão inválidos.

De acordo com a *Kaspersky*, existem duas principais categorias de *ransomware* que podem ser diferenciados da seguinte forma:

- ***Ransomware* de bloqueio**: impede que os usuários realizem funções básicas no dispositivo, como acesso à área de trabalho, funções de mouse e teclado. O *malware* de bloqueio geralmente evita a criptografia dos arquivos importantes em prol do simples bloqueio.
- ***Ransomware* de criptografia**: o objetivo deste tipo é realizar a criptografia de dados importantes no dispositivo, documentos, fotos, vídeos, gerando uma sensação de pânico, pois não é possível acessar esses arquivos.

3.4 Meios de prevenção

Os ataques virtuais e as ameaças cibernéticas são grandes desafios para as empresas, mas eles podem ser reduzidos conhecendo os vários tipos de protocolos, explorações, ferramentas e recursos usados por cibercriminosos, pois ao saber onde e como esperar ataques é possível que você crie medidas preventivas para proteger seus sistemas. Quase todas as organizações modernas exigem em sua infraestrutura de TI, no mínimo, uma rede de

computadores e seus ativos que compõem sua estrutura de conectividade, além de outros dispositivos móveis que completam uma arquitetura tecnológica. Infelizmente, embora esses dispositivos e aplicativos ofereçam um grande benefício para a empresa, eles também podem representar um risco. Basta uma gestão ineficiente dos ativos ou um funcionário clicar em um link malicioso que, em seguida, os cibercriminosos obtêm acesso à sua rede e infectam seus sistemas.

Implementar controles e processos de segurança que possam mitigar os ataques tornando sua empresa um alvo difícil são fundamentais no âmbito da prevenção. Além de adotar uma abordagem de defesa em profundidade para mitigar os riscos por meio de toda a gama de ataques cibernéticos em potencial, dando à sua empresa mais resiliência para lidar com ataques que usam ferramentas e técnicas mais personalizadas.

Informações publicadas para consumo aberto devem ser filtradas sistematicamente antes de ser liberada para garantir que qualquer coisa de valor para um invasor seja removida. O treinamento, a educação e a conscientização do usuário são importantes, todos os seus usuários devem entender como as informações publicadas sobre seus sistemas e operação podem revelar possíveis vulnerabilidades. Eles precisam estar cientes dos riscos de discutir tópicos relacionados ao trabalho nas mídias sociais e do potencial de serem alvo de ataques cibernéticos e ataques de *phishing*. Eles também devem entender os riscos para o negócio de liberar informações confidenciais em conversas gerais, chamadas telefônicas não solicitadas e destinatários de e-mail.

O processo de criptografia de dados também é bastante importante, onde se converte as informações em um formato que não pode ser lido por uma pessoa não autorizada. Somente uma pessoa confiável, autorizada com a chave secreta ou uma senha, pode descriptografar os dados e acessá-los em sua forma original. A criptografia em si não impede que alguém intercepte os dados, mas ela pode impedir uma pessoa não autorizada de exibir ou acessar o conteúdo. Existem programas de software que são usados para criptografar arquivos, pastas e até mesmo unidades inteiras.

Controles de acesso de usuário bem implementados e mantidos restringirão os aplicativos, privilégios e dados que os usuários podem acessar. A configuração segura pode remover software desnecessário e contas de usuário padrão, além de também pode garantir que as senhas padrão sejam alteradas e que todos os recursos automáticos que possam ativar malware imediatamente sejam desativados.

Diante dessas informações e com todo esse aumento de ataques e riscos à Segurança da Informação nas organizações, é necessário a implementação de medidas para diminuir problemas que possam acontecer, dentre as mais eficazes podemos destacar:

- **Programa de Segurança da Informação:** com políticas e diretrizes para o uso de dados e sigilo de documentos, níveis de permissionamento para uso de recursos e ativos de Tecnologia da Informação, normas de conduta dos colaboradores ao utilizar sistemas e dispositivos que façam parte da cadeia produtiva da organização, manter essas políticas atualizadas e revisadas periodicamente.
- **Treinamento periódico**: aos colaboradores e outros que utilizem os sistemas e dispositivos da organização, capacitando-os a identificar possíveis ataques de engenharia social, *phishing e* como agir nos casos de um ataque cibernético, além de abordar métodos e táticas de prevenção em relação ao uso dos recursos de Tecnologia da Informação.

- **Controle de acesso:** restringir o acesso com base nas funções de cada colaborador, atribuindo permissões específicas para cada função existente, essa prática permite que usuários acessem somente arquivos e sistemas que são exigidos pela sua função ou departamento na organização. Definir conta de acesso individual para cada colaborador aumenta a segurança e ajuda a identificar o ponto de origem no caso de algum ataque interno;
- **Requisitos de senhas e autenticação:** as senhas são a primeira defesa para impedir acessos não autorizados aos sistemas, dados e informações. Exigir que as senhas tenham tamanho e complexidade e que seja realizado a alteração a cada período, habilitar algum tipo de autenticação multifatorial aumenta muito a segurança no caso de uma credencial ter sido comprometida;
- **Política de realização de *backup*:** ter um *backup* completo, atualizado, garantindo que ele esteja íntegro, protegido e preferencialmente em nuvem, caso seus arquivos sejam perdidos ou corrompidos ele pode ser a solução para a continuidade dos negócios da organização, apesar desta prática não coibir um ciberataque como o de *ransomware*, pode ser a solução caso seja vítima;
- **Atualização do sistema:** manter os sistemas operacionais dos dispositivos sempre atualizados com as atualizações do fabricante que visam corrigir vulnerabilidades conhecidas para evitar que ataques explorem essas vulnerabilidades, isso diminui as chances de os atacantes obterem sucesso;
- **Privilégios administrativos:** atentar-se aos privilégios administrativos de usuários e *softwares* que solicitam esses privilégios no momento da instalação.
- **Uso de antivírus:** fazer o uso de um bom antivírus com base de dados atualizada ajuda na proteção, impedindo que aplicativos desconhecidos sejam executados sem autorização do usuário, detectando a presença de vírus e ameaças em unidades removíveis e fornece segurança adicional no momento da navegação em páginas da internet;
- ***Firewall*:** fazer o uso de *firewall*, configurado de maneira correta e com monitoramento constante do fluxo de dados ajuda a proteger e identificar possíveis falhas e corrigi-las;
- **Portas:** realizar periodicamente a varredura de portas abertas nos sistemas e desabilitar caso não estejam em uso, grande parte dos incidentes bem-sucedidos se dão por conta de portas abertas que até então era desconhecido pelos administradores da rede;
- **Licenças de sistemas:** fazer o uso de licenças genuínas, mesmo com todas as evidências de ciberataques ainda existem empresas que utilizam de *softwares* piratas para utilização de *software* e aplicativos, correndo um grande risco de invasão e ataque.
- **Monitoramento estratégico:** monitorar o uso da infraestrutura e recursos de Tecnologia da Informação, aplicando medidas e realizando mudanças quando necessário, de modo a garantir a disponibilidade dos recursos de *hardware* e *software*, evitando indisponibilidades, interrupções e falhas que possam causar prejuízos;
- **Plano de Continuidade de Negócios (PCN):** Definir um plano de continuidade de negócios, que oriente a organização a responder, recuperar e restaurar a um nível que minimize os impactos do ataque para que a empresa retorne à condição operacional;

4 Considerações finais

O desenvolvimento do presente artigo possibilitou uma análise dos principais ataques que ocorrem na atualidade ocasionando o vazamento e exposição dos dados, descrevendo os mais comuns e explorados por cibercriminosos, e de como é de extrema importância medidas

de prevenção, deixando evidente a necessidade de treinamentos e métodos que podem ser adotados para manter os dados seguros, sejam eles dados pessoais ou empresariais. Por conta disso, a ideia de melhores práticas, capacitação do colaborador, evidenciando meios de prevenção para que se possa garantir a proteção dos dados de uma forma eficaz no dia a dia, foram passadas como soluções a serem adotadas na questão da segurança dos dados.

Conclui que desta forma que, o principal elo, mais importante e ao mesmo tempo mais vulnerável na segurança da informação remete-se ao indivíduo, o fator humano, e pode ser preciso e confiável mediante a capacitação com instrução e treinamento.

O presente artigo atua como um guia para estudantes e público em geral, interessados na área de Segurança da Informação e proteção de dados.

REFERÊNCIAS

ABNT (Associação Brasileira de Normas Técnicas) NBR ISO/IEC 27002: **Tecnologia de informação: Técnicas de segurança** - Código de prática para controles de segurança da informação. 2 ed. Rio de Janeiro: ABNT, 2013. Citado na página 3.

BEAL, Adriana. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. São Paulo: Atlas, 2003. Citado na página 5.

Brasil sofreu mais de 33 milhões de tentativas de ransomware em 2021. Disponível em: https://tiinside.com.br/18/02/2022/brasil-sofreu-mais-de-33-milhoes-de-tentativas-de-ransomware-em-2021/. Acesso em: 01 mai. 2022. Citado na página 8.

Brasileiros são principais alvos de ataques de phishing no mundo. Disponível em: https://www.kaspersky.com.br/blog/brasileiros-maiores-alvos-phishing-mundo/17045/. Acesso em: 18 abr. 2022. Citado na página 6.

Engenharia social - Definição. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 20 abr. 2022. Citado na página 4.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar**. São Paulo: Pearson Makron Books, 2003. Citado nas páginas 3 e 4.

O aumento do ransomware – exemplos mais notáveis. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware-threats-an-in-depth-guide. Acesso em: 27 mar. 2022. Citado na página 8.

O que é engenharia social e por que é uma ameaça em 2022? Disponível em: https://pt.safetydetectives.com/blog/o-que-e-engenharia-social-e-por-que-e-uma-ameaca-tao-grande/. Acesso em 30 mar 2022. Citado na página 5 (Figura 2).

Quais são os diferentes tipos de phishing? Disponível em: https://www.trendmicro.com/pt_br/what-is/phishing/types-of-phishing.html. Acesso em: 03 abr. 2022. Citado na página 6.

SÊMOLA, M. **Gestão da Segurança da Informação**. **Uma visão Executiva.** Rio de Janeiro: Elsevier, 2013. Pag. 1 e 37. Citado na página 2.

SILVA, Denise R. P. da. STEIN, Lilian M. **Segurança da informação: uma reflexão sobre o componente humano**. Ciências & Cognição. 2007;
Disponível em: http://www.cienciasecognicao.org/pdf/v10/m346130.pdf. Acesso em: 12 fev. 2022. Citado na página 2.

Izaias Maia Vieira
Matheus Wilson Ramos Pereira

MÉTODOS MAIS UTILIZADOS NO VAZAMENTO DE DADOS NAS ORGANIZAÇÕES E MEIOS DE PREVENÇÃO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Segurança da informação.

Americana, 20 de junho de 2022

Banca Examinadora:

Daives Araken Bergamasco (**Presidente**)
Doutor
FATEC - Faculdade de Tecnologia de Americana

Rogério Nunes de Freitas (**Membro**)
Mestre
FATEC - Faculdade de Tecnologia de Americana

Tiago Rebecca (Membro)
Mestre
FATEC - Faculdade de Tecnologia de Americana