Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

A importância da Segurança da Informação no Home Office

Vitoria do Nascimento Rodrigues, Samuel da Mata Proença

Orientador: Daives Arakem Bergamasco

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana) Ministro Ralph Biasi

Americana – SP – Brasil

vitoria.rodrigues5@fatec.sp.gov.br,
samuel.proenca2@fatec.sp.gov.br
Orientador: daives.bergamasco@fatec.sp.gov.br

Abstract. Information security has become increasingly important and essential in our daily lives, due to the increase in information traffic in the virtual environment. In view of this, the need arose to protect shared data in the virtual environment, which in turn became more vulnerable to attacks and theft. Throughout this evolution, it was necessary to adapt technological resources according to the raw material provided by the environment and the situation in which we live, for example the SARS-CoV-2 (Covid-19) pandemic that forced several organizations to adopt the "home office" work modality to contain the spread of the virus.

Keywords: Information Security; Protect; Pandemic; Home Office.

Resumo. A segurança da informação se tornou cada vez mais importante e essencial em nosso cotidiano, em razão do aumento do tráfego de informações no ambiente virtual. Em vista disso, surgiu a necessidade de se proteger os dados compartilhados no meio virtual, que, por sua vez se tornou mais vulnerável à ataques e roubos. Ao longo de toda esta evolução, foi necessário adaptar os recursos tecnológicos de acordo com a matéria prima fornecida pelo meio ambiente e situação em que vivemos, em exemplo a pandemia do SARS-CoV-2 (Covid-19) que obrigou diversas organizações adotarem a modalidade de trabalho "home office" de forma a conter o avanço do vírus.

Palavras-chave: Segurança da Informação; Proteger; Pandemia; Home Office.

1. Introdução

Visto que a tecnologia se tornou cada vez mais presente em nossas vidas, este artigo aborda a importância da segurança da informação atualmente, priorizando a forma de trabalho "Home Office". Considerando que passamos por constantes mudanças na época e meio ambiente em que vivemos, citaremos a pandemia do Covid-19 (SARS-CoV-2), que no ano de 2020 induziu diversas organizações a se adaptarem às novas tecnologias e métodos para não ficar para trás mediante uma crise pandêmica e econômica que atingiu o mundo inteiro.

Pode-se dizer que a tecnologia em conjunto com a internet é um elemento extremamente importante que traz benefícios para quem a utiliza, facilitando deste modo processos e diminuindo prazos, entretanto, possui também seus males. De acordo com isso, a segurança da informação existe principalmente para assegurar que a tecnologia e a informação sejam manuseadas da forma correta, implementando políticas de segurança que garantam a confidencialidade, integridade e disponibilidade da informação.

2. Objetivos

Neste artigo será abordado a importância da segurança da informação no meio de trabalho “Home Office”, que aumentou exponencialmente nos últimos anos mediante a pandemia do Covid-19 (SARS-CoV-2). Dado o meio de trabalho "Home Office", todos estamos vulneráveis a qualquer tipo de ataque e roubo de informações, desta forma citaremos alguns tipos de ataque e o quão necessário é a implementação de Políticas de Segurança e a capacitação dos profissionais na área.

3. Desenvolvimento

3.1. Conceito de Internet

A internet é, sem dúvidas, uma das melhores invenções do século XX. Desde seu surgimento, foi transformando cada vez mais o modo como vivemos e nos relacionamos.

O surgimento da internet se deu durante a Guerra Fria em 1957, mediante a necessidade dos soldados norte-americanos se comunicarem com a outra parte do exército que estava em locais afastados. Além de ter sido criada com o intuito de encontrar uma maneira facilitadora de troca de informações, a internet foi criada também com o objetivo proteger as informações de um ataque nuclear.

Além da utilização na guerra para proteção e troca de informações, é possível dizer que por outro lado a princípio a ideia da criação da internet era baseado em apenas conectar os mais importantes centros de pesquisa dos Estados Unidos da América, porém nos anos 70 começou a ser utilizada pela comunidade acadêmica mundial e em 1975 teve as primeiras ligações internacionais que mudaram a perspectiva do mundo.

Com esse aumento na utilização deste novo recurso, houve um alastramento da internet que acabou possibilitando a mesclagem do mundo real (ambiente físico) com o mundo virtual.

Segundo a Equipe Brasil Escola, podemos afirmar que:

> "A Internet tem revolucionado a comunicação mundial ao permitir, por exemplo, a conversa entre usuários a milhares de quilômetros pelo preço de uma ligação local. O grande número de pessoas que a utilizam também é responsável pelo maior problema da rede: o congestionamento e a lentidão no acesso aos serviços. Coma Internet surge a expressão ciberespaço, que significa o espaço virtual e sem fronteiras, no qual circulam os milhares de informações veiculadas na rede.”

Graças ao aumento dessa nova forma de comunicação, hoje podemos fazer tudo que imaginarmos no meio virtual, dependendo do caso, é possível refletir também no ambiente físico. Esse novo recurso acabou possibilitando o trabalho de remoto de qualquer lugar desde que haja acesso à internet. Entretanto, isto pode ser também um empecilho a quem não está acostumado com este tipo de recurso.

3.2. Conceito de Segurança da Informação

Em primeiro lugar, o que é a informação? A informação é um conjunto de dados organizados que podem ser considerados um ativo de valor e que deve ser protegido por meio de políticas e regras. Na época atual em que vivemos, com o grande avanço da tecnologia e o aumento da transferência de dados via internet, gera-se uma certa preocupação sobre a segurança de todos esses dados, com isso a segurança da informação se torna cada vez mais importante e necessária neste ambiente virtual.

A Segurança da Informação compreende um conjunto de normas, procedimentos e políticas que possuem o objetivo de proteger e preservar o recurso da informação e de sistemas de informação. A Segurança da Informação agora é algo indispensável de ser usado nas empresas/organizações, esta tem o principal objetivo assegurar que todos os dados empresariais/organizacionais permaneçam corretamente armazenados e protegidos, tornando-os sigilosos. Em resumo, a segurança da informação visa impedir que qualquer pessoa de fora da empresa ou pessoas que não tem a devida autorização possa acessar, vazar e ou até mesmo roubar dados que podem muitas vezes acabar sendo prejudiciais para a empresa.

> "Diferente do que muitos pensam, a segurança da informação não está relacionada apenas a computadores, celulares, sistemas e arquivos digitais. Além do mundo da informática, segurança da informação pode incluir pessoas, documentos impressos e ambientes." [ACADI-TI, 2020?].

Os primeiros registros históricos da Segurança da Informação surgiram nos anos 90, junto com a necessidade de se proteger os dados armazenados no ambiente virtual. A segurança da informação foi de fato aplicada mediante a introdução dos primeiros antivírus. Junto com a criação do software de antivírus houve também a criação da primeira versão do padrão BS7799, que é uma norma de segurança Britânica e que deu origem as normas atuais como a ISO/IEC 27002, essas normas contém as melhores práticas para ajudar com o gerenciamento da Segurança da Informação.

Como base, a segurança da informação possui os seguintes critérios:

> "Confidencialidade – Falhas neste critério podem expor dados estratégicos da organização para concorrentes, ou então oportunizar um vazamento de dados de clientes realizado por hackers. Além de severos prejuízos financeiros, este tipo de situação compromete muito a imagem da empresa no mercado, evidenciando as falhas de segurança para o público.
>
> Integridade – A integridade envolve o acesso às informações por inteiro. Um erro no servidor, por exemplo, pode corromper determinados arquivos importantes. Sem a prática rotineira de backups, as funções da empresa podem ficar comprometidas.
>
> Disponibilidade – Os dados precisam estar acessíveis quando forem requisitados, principalmente para garantir a agilidade dos processos. Falhas na segurança da informação podem impedir a disponibilidade, como nos casos de ataques de sequestro de dados (ransomware).
>
> Autenticidade – Há um grande risco de fraudes por processos falhos de garantia de autenticidade de transações, e isso pode causar problemas graves a longo prazo. No uso de informações de cartões de crédito, por exemplo, podem ocorrer a clonagem e até mesmo a invasão de dados." [ACADI-TI, 2020].

A aplicação da segurança da informação tem extrema importância para evitar a perdas de dados, tendo como fundamento a utilização normas, métodos e políticas de segurança para uma análise adequada na empresa descobrindo todo tipo de falha e vulnerabilidade que possa acarretar prejuízos futuros, podendo ser falhas na plataforma digital ou até mesmo físicas.

No momento atual em que vivemos, com a maioria das empresas adotando formas de trabalho em Home Office, a Segurança da Informação precisa ser mais ainda aplicada nos meios digitais. Com o crescimento deste modo de trabalho os criminosos cibernéticos podem avaliar como uma vulnerabilidade, já que o usuário está sem monitoramento e podem se aprimorar em técnicas que podem afetar o usuário e consequentemente a organização.

4. Engenharia Social como problema na Segurança da Informação

4.1. O que é?

No que se refere a Segurança da Informação, pode-se dizer que a Engenharia Social é uma técnica praticada virtualmente por pessoas que são denominadas "criminosos cibernéticos" e que visam manipular os usuários da internet para conseguir obter informações confidenciais do próprio usuário ou da organização considerada alvo.

Nesta tática os criminosos cibernéticos possuem como principal propósito usar diferentes métodos para convencer suas vítimas a divulgarem informações, podendo se beneficiar com elas ou não. Dados as ocorrências atuais, é possível dizer que uma parte desses criminosos cibernéticos realizam esses tipos de ataque por diversão, tendo em consideração apresentar o que é capaz de fazer.

4.2. Como a engenharia social funciona?

> *"A engenharia social funciona aproveitando os vícios cognitivos das pessoas. Quem usa engenharia social se apresenta como uma pessoa simpática, confiável ou com autoridade para ganhar a confiança da vítima. Uma vez que o invasor ganha essa confiança, a vítima é manipulada para entregar informações privadas."* [Bodnar, Danielle. Avast, 2020].

O principal alvo destes criminosos são empresas de grande porte, em razão de que estas possuem uma grande quantidade de dados confidenciais, entretanto empresas pequenas também podem ser um alvo fácil, visto que possuem diversos dados que são manipulados por usuários que nem sempre percebem o verdadeiro valor dos dados e não sabem propriamente como defendê-los ou se quer manipulá-los da forma correta, podendo ser considerado uma vulnerabilidade.

Há diversos tipos de ataques cibernéticos que agem de forma camuflada e que servem como ponte entre a rede interna da organização e o computador da vítima sem ser detectado, por isso é extremamente importante que a empresa invista sempre na segurança dos seus ativos e no treinamento de seus funcionários de forma a evitar estes ataques.

O trabalho remoto facilita esses ataques cibernéticos por engenharia social no "home office" pois a maioria dos funcionários ao operar a máquina da empresa deixam de lado as políticas de segurança pré-determinadas pela empresa, ou seja, são menos cautelosos pois não estão sendo "monitorados". Visando agilizar os processos da empresa, é muito comum o uso de dispositivos pessoais no home office, isso pode ser um potencial de abertura de portas para informações confidenciais da organização. Em exemplo, o uso da máquina da empresa/organização para baixar jogos e aplicativos interativos que não "rodariam" em sua máquina pessoal, isto é uma grande falha principalmente se não validar a origem.

5. Conceito de Home Office

A tradução da expressão Home Office significa “escritório em casa”, entretanto não precisa ser executado necessariamente em “casa”, devido a isso pode-se dizer que existem outros termos mais precisos para definir essa modalidade de trabalho, como por exemplo Trabalho Remoto, Teletrabalho, Trabalho à Distância ou Trabalho Portátil.

> " O Home Office surgiu nos Estados Unidos, quando tecnologias como o computador, a internet e o celular foram popularizados. Isso possibilitou que qualquer um tivesse sua própria estação de trabalho na sua casa. Para algumas pessoas pode ser difícil imaginar, mas por muito tempo, o custo dessas tecnologias as tornou inacessíveis a maior parte das pessoas e seu acesso era limitado a ambientes corporativos. À medida que esse custo foi caindo, o Home Office foi crescendo.
>
> Além do avanço e da popularização da internet e dos computadores pessoais, o surgimento de ferramentas, como programas e softwares permitiram que pessoas pudessem trabalhar remotamente, trabalhar de casa, de aeroportos ou de onde preferissem, sem prejuízo à comunicação ou à produtividade da equipe.” [PortalISO, 2020]”

Atualmente, a prática do home office tem crescido em todo o mundo e se mostrado muito importante devido as condições atuais em que vivemos, tanto quanto pandêmicas quanto econômicas.

Pode-se dizer que a pandemia do Cóvid-19 (SARS-CoV-2) foi o principal fator que impulsionou a adoção desse modo de trabalho, levando em consideração a transmissão do vírus que ocorria de forma simples e com alto nível de transmissão, podendo ser fatal dependendo da pessoa. Essa pandemia desenrolou-se de forma rápida e inesperada, de acordo com a gravidade inicial isso acabou estabelecendo um grande aumento de empresas que adotaram este modo de trabalho.

Com isso elas acabaram cortando grande parte dos gastos por manter seus prédios em funcionamento, possibilitando também que seus funcionários tenham uma maior flexibilidade de trabalho desde que tenham acesso à internet. Inicialmente as empresas acreditaram que seria temporário, porém muitas delas aprovaram este modo de trabalho e acabaram implementando de forma fixa, visto que reduziram custos e produziram de acordo com o esperado.

6. Vulnerabilidade no Home Office

Com o aumento da utilização do Home Office como meio de trabalho, as empresas tiveram que se adequar no mercado de trabalho, por um lado isso trouxe pontos positivos, mas também alguns pontos negativos, dentre esses, muitos estão relacionados com os dados e a segurança digital da empresa.

Dado a possibilidade de trabalhar no Home Office, é possível afirmar que houve um aumento considerável de pessoas conectadas com a internet, é comum que as empresas forneçam ferramentas para que seus funcionários possam trabalhar, em sua maioria são disponibilizados notebooks, onde o usuário tem permissão de acesso aos sistemas da empresa. Entretanto, dependendo do porte da empresa nem sempre isso é possível, dando a possibilidade e a liberdade do funcionário utilizar sua própria máquina para manipular as informações da empresa e executar seu trabalho.

Devido a isso ocorreu um grande aumento de ataques cibernéticos nas empresas, independentemente de seu porte, se há um alto fluxo de informações ou não, atualmente os criminosos aumentaram seus ataques buscando por pontos que não possuem uma gerência adequada dos dados e métodos de prevenção, ou seja, que contém certas vulnerabilidades.

Mediante as ocorrências, é possível dizer que a maioria das empresas que não buscam se prevenir por questões financeiras e que não consideram o gasto em prevenção como "um bom investimento" estão mais vulneráveis a este tipo de ataque pois não fornecem um treinamento adequado para seus funcionários mostrando como se precaver contra esses ataques no Home Office. A prevenção sempre será uma boa forma de evitar os ataques, principalmente quando se há a possibilidade de conectar suas contas pessoais ou hardwares não autorizados nas máquinas da empresa.

Dado as informações, listaremos neste artigo os 3 principais tipos de ataques cibernéticos que ocorrem frequentemente nas organizações em dias atuais com o grande avanço da tecnologia e aumento do home office. Levando em consideração a citação anterior em que o método de trabalho home office pode ser considerado uma vulnerabilidade para determinadas empresas, visto que nem sempre há como monitorar o que o usuário está fazendo em seu local de trabalho particular.

7. Tipos de Ataque no Home Office

7.1. Phishing

O conceito do nome Phishing, vem derivado da palavra "fishing" na língua inglesa. O termo que dá o nome desse tipo de ataque cibernético consiste em um tipo de ato em que a intenção é "pescar" informações da vítima de forma online.

É possível afirmar que uma das práticas principais deste tipo de ataque é através da criação e-mails falsos que buscam roubar dados importantes da vítima (o alvo pode ser tanto uma pessoa comum quanto uma empresa), tais como logins de acesso, dados da conta bancária e até mesmo informações pessoais, tudo isso junto com a tentativa de instalar softwares maliciosos no computador da vítima para tornar mais fácil o roubo dos demais dados. *"São literalmente "fisgadas" por um chamariz, a palavra phishing não existe, mas é utilizada pela semelhança com fishing (pescar) em inglês. A ideia da palavra é "pescar a vítima por meio de informações falsas"* [Kovacs, Leandro. Tecnoblog, 2020].

Para que os criminosos consigam obter os dados da vítima, o e-mail é certamente bem descrito e enviado para a vítima com métodos que induzem o destinatário acreditar no e-mail e a passar as informações sem questionar e duvidar, geralmente o conteúdo da mensagem são referentes a confirmações bancárias ou até mesmo da própria empresa onde a vítima trabalha, no qual ao clicar em um link contido na mensagem o usuário é redirecionado para uma outra página que contém um formulário a ser preenchido com os dados a serem roubados ou até mesmo através do download de um software malicioso, que age discretamente roubando informações digitadas no computador pelo usuário.

Com o frequente uso e aumento do meio de trabalho de home office pelas empresas, o cuidado das empresas com este método deve ser redobrado. É considerado uma grande vulnerabilidade quando não se há conhecimento o suficiente para que possa identificar que possivelmente está se tornando uma vítima desse tipo de ataque.

7.2. Backdoor

De forma simples, o backdoor é um tipo de malware que consiste em métodos que possibilitam os criminosos virtuais acessarem remotamente os computadores das vítimas para obter acesso aos dispositivos e consequentemente ao sistema.

O backdoor está agrupado com aplicativos e arquivos gratuitos, isto pode ser

considerado uma vulnerabilidade no home office pois ao baixar um programa sem a autorização do proprietário pode servir como porta de acesso desse conteúdo malicioso ao sistema que contém os dados confidenciais da organização. *"Essas invasões são capazes de fazer com que dados empresariais sigilosos sejam expostos ou usados como forma de extorsão, por exemplo"* [Value Host, 2022].

Pode se dizer que no backdoor o cibercriminoso consegue acessar os recursos dentro de uma aplicação, como por exemplo os servidores de arquivos da organização, essa invasão faz com que ele tenha permissão de manipular comandos do sistema e fazer update de códigos maliciosos.

Muitas das vezes o funcionário por estar em "home office" acaba baixando a guarda e com isso realiza a instalação de aplicativos na máquina que em sua compreensão podem ser de bom uso, porém se não baixado em sites confiáveis podem vir com este conteúdo malicioso.

7.3. Quid pro quo

"Um ataque quid pro quo é caracterizado por uma "dar e receber" intercâmbio. Significa literalmente algo por algo." [Nadeem, Salman. Mailfence, 2018].

Esta técnica de ataque é semelhante ao Phishing, no qual o criminoso encaminha e-mails para a vítima, mas nesse caso ele visa se passar por alguém que irá ajudar ou fornecer algo para o alvo em troca de que ofereça alguma informação que possa ser considerada como benefício, de preferência logins e credenciais que permitem acesso aos dados da organização. Geralmente o atacante analisa as vulnerabilidades, antes de qualquer ataque

No exemplo do Home Office, visto que a vítima pode estar sozinha em um local distante da empresa, o atacante pode se aproveitar informando que por algum acaso a máquina está com problemas tecnológicos e oferecendo assistência remota para concertar, nisso pede para que a vítima passe os dados de acesso e com isso sem consciência ela permite que o criminoso tenha acesso aos sistemas da empresa. Como o funcionário não está fisicamente na empresa, é facilmente de manipular pois não está de fato vendo o que está acontecendo.

8. Prevenção

8.1. Conscientização e Criação de Políticas de S.I.

Pode-se dizer que nem sempre é tão fácil reconhecer e evitar um ataque de engenharia social, principalmente quando trabalhamos em Home Office e deixamos de lado a cautela, com isso estamos mais propensos a ser manipulados, podendo ser a próxima vítima de um ataque de engenharia social. É de grande importância que as organizações invistam em treinamentos e métodos de prevenção pois é melhor gastar com um investimento do que com prejuízos maiores que poderiam ter sido evitados.

Atualmente com o avanço da Tecnologia é possível obter treinamentos rápidos que podem causar um bom resultado, podendo ser um treinamento on-line diretamente com um responsável pela área de Segurança da Informação ou até mesmo através de algum vídeo informativo, vale a pena ressaltar que um funcionário bem treinado saberá questionar de fato se algo possui uma confidencialidade integra ou não e assim encaminhar ao responsável pela análise mais aprofundada.

Como prevenção é extremamente importante conferir a fonte da mensagem, ainda mais quando não se está presencial na empresa, acompanhando ao vivo o que ocorre fisicamente lá. No Home Office sem o contato com o restante da equipe é mais fácil ainda de ser manipulado,

entretanto, com a conferência da origem da mensagem é possível dar seguimento ou denunciá-la ao responsável.

Ao receber um e-mail de aparência suspeita, deve-se conferir o endereço de e-mail do remetente, confirmando o domínio se está de acordo com os padrões enviados pela empresa. A proteção dos dispositivos com antivírus e sistemas que monitoram/barram certas ações dos usuários é crucial para a segurança dos dados da organização, visto que a nossa presença online é um dos principais fatores que levam os criminosos a atacarem e analisarem as vulnerabilidades.

Como garantia da segurança dos dados, tanto a empresa quanto os funcionários devem assegurar que todos os dados e as informações geradas e passadas por eles estão de acordo com as normas e Políticas de S.I. Muitas dessas são criadas e estabelecidas pela LGPD Lei nº 13.709/2018 (Lei Geral de Proteção de dados Pessoais).

Esta Lei tem como principal função esclarecer como que os dados pessoais informados serão tratados e armazenados semelhante a lei GDPR (General Data Protection Regulation) que é a lei europeia sobre proteção de dados. A LGPD assegura que os dados informados possuem a privacidade adequada e são devidamente protegidos, estabelecendo regras sobre o tratamento dessas informações. Na LGPD é tratado também a questão do manuseio dos dados, no qual devem ter o consentimento do dono para poder manuseá-los.

8.2.Termo de Responsabilidade

Empresas que disponibilizam o uso do Home Office para seus funcionários precisam ainda mais manter seus dados seguros, mediante isso é possível dizer que um método válido de prevenção pode ser a implementação de um termo de responsabilidade sobre o uso da informação, sendo direcionado aos funcionários para que estejam cientes dos riscos e as normas que devem ser cumpridas. A LGPD é uma lei que facilita o compreendimento e implementação desses tipos de normas, visto que ela foi uma grande conquista a todos que desejam seus dados seguros.

Portanto, mediante toda essa tecnologia e a possibilidade de trabalhar em Home Office é essencial ter um bom planejamento que esteja de acordo com a LGPD (Lei Geral de Proteção de Dados), pois além do cumprimento da lei deve-se a preservação das informações que envolvam os titulares dados e por consequência a empresa que os tem.

Um bom planejamento seria a realização de backups de segurança e barrar o registro de fotos da tela do computador, visto que é uma forma de evitar o roubo de dados.

8.3. Proteção contra o Phishing

Para garantir uma maior proteção contra esse método de ataques da Engenharia Social, é recomendado acompanhar acontecimentos tecnológicos e buscar por dicas que ajudem a se prevenir contra e não ter suas informações roubadas.

É extremamente importante ficar atento com o tipo de e-mail que recebemos, sendo necessário validar sempre a origem dele, visto que o principal meio de ataque phishing é através de e-mails e a trocas desse tipo de mensagem é ainda maior no home office por conta da distância.

Dado a situação é necessário orientações internas informando seus funcionários para que nunca acessem seus e-mails pessoais nos computadores oferecidos pela empresa para o trabalho remoto, também não fazer cadastros em serviços com o e-mail empresarial, assim evitando que informações da empresa sejam roubadas. É de extrema importância a checagem

da origem do e-mail, pois a maioria das empresas como por exemplo Bancos, não exigem que o usuário informe seus dados pessoais por e-mail, geralmente esse tipo de e-mail é um golpe e pode ser alguém tentando roubar seus dados.

8.4. Proteção contra Backdoor

Sabemos que o Backdoor é um problema muito grave para as empresas, podendo liberar o acesso para que os ciberciminosos invadam remotamente os computadores e roubem os dados das empresas.

Como a maioria das empresas fornecem notebooks para que seus funcionários possam trabalhar em Home Office, como forma de prevenção é recomendado a instalação de um Firewall na máquina, pois com esse recurso estando bem configurado é possível estabelecer uma segurança na rede e tráfego de dados via internet, assim monitorando as portas de acesso e a entrada e a saída dos dados permitindo quais dados podem passar e quais serão bloqueados.

O Firewall contém um conjunto de normas e regras de segurança, por isso é extremamente importante que este recurso seja instalado e enviado junto com o notebook para o funcionário e serem feitas atualizações frequentes para que mantenha a segurança do dispositivo.

8.5. Proteção contra Quid pro quo

O ataque Quid pro quo é semelhante ao Phishing, pode-se dizer que uma prevenção considerável para isto é validar se realmente estão com algum problema e definir protocolos de ação mediante a isso, visto que o atacante tentará se passar por alguém que está oferecendo assistência.

É de extrema importância validar com os colaboradores da empresa como será o sistema de trabalho e conscientizar que não se deve divulgar informações para qualquer pessoa, definindo uma hierarquia com controle de acesso.

Conclusão

A tecnologia em conjunto com a internet é um elemento que realmente traz benefícios para quem a utiliza, porém quando manuseada da forma correta, garantindo principalmente a confidencialidade e integridade de informação, sem prejudicar o seu proprietário. Com os avanços tecnológicos e a adoção do home office é possível dizer que esses ataques irão aumentar cada vez mais, necessitando ainda mais a capacitação de profissionais na área para proteger e suportar a alta demanda de informações que são processadas nesse ambiente virtual.

O investimento em prevenção e conscientização sempre será um bem necessário a quem está disposto a evitar prejuízos.

Referências

ADIL, Josué. **Segurança da informação: o que é e qual sua importância.** ACADI-TI, [s.d.]. Disponível em: https://acaditi.com.br/seguranca-da-informacao-o-que-e-e-qual-sua-importancia/. Acesso em: 28 fev. 2022.

Blockbit. **Você sabe como evitar backdoors?** Blockbit, [s.d.]. Disponível em: https://www.blockbit.com/pt/blog/como-evitar-backdoors/. Acesso em: 2 nov. 2022.

BODNAR, Danielle. **Engenharia social e como evitá-la**. Avast Academy, 2020. Disponível em: https://www.avast.com/pt-br/c-social-engineering. Acesso em: 12 mai. 2022.

Cisco. **O que é um firewall?** Cisco, [s.d.]. Disponível em:https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html. Acesso em: 2 nov. 2022.

Equipe Brasil Escola. **INTERNET: Internet, a história da Internet, surgimento da Internet, a Internet no Mundo, o que é internet, o surgimento da internet no Brasil, a internet no Brasil**. Monografias Brasil Escola, [s.d.]. Disponível em: https://monografias.brasilescola.uol.com.br/computacao/internet.htm. Acesso em: 9 mar. 2022.

Equipe RH Portal. **Funcionários em home office são os principais alvos de hackers**. RH Portal, 2020. Disponível em: https://www.rhportal.com.br/artigos-rh/funcionarios-em-home-office-sao-os-principais-alvos-de-hackers/. Acesso em: 20 jun. 2022.

K, Fabiana. **Backdoor: como funciona uma invasão cibernética nas empresas?** Hostone, 2021. Disponível em: https://blog.hostone.com.br/o-que-e-backdoor/. Acesso em: 22 ago. 2022.

Kapersky. **Engenharia social - Definição**. Kapersky, [s.d.]. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 20 abril. 2022.

KOVACS, Leandro. **O que é backdoor em computação?** Tecnoblog, 2021. Disponível em: https://tecnoblog.net/responde/o-que-e-backdoor-em-computacao/. Acesso em: 05 ago. 2022.

KOVACS, Leandro**. O que é phishing?** Tecnoblog, 2020. Disponível em: https://tecnoblog.net/responde/o-que-e-phishing/. Acesso em: 25 jun. 2022.

NADEEM, M Salman. **Engenharia social: ataques quiproquó**. Mailfence, 2022. Disponível em: https://blog.mailfence.com/pt/engenharia-social-ataques-quiproquo/. Acesso em: 19 ago. 2022.

NortonLifeLock. **O que é engenharia social?** NortonLifeLock, [s.d.]. Disponível em: https://br.norton.com/blog/emerging-threats/what-is-social-engineering. Acesso em: 20 abril. 2022.

NUÑEZ, Benigno. **TRABALHO EM HOME OFFICE: Análise sobre o trabalho em home office**. Brasil Escola, [s.d.]. Disponível em: https://meuartigo.brasilescola.uol.com.br/direito/trabalho-em-home-office.htm#:~:text=A%20partir%20das%20décadas%20de,trabalho%20na%20modalidade%20home%20office. Acesso em: 16 mar. 2022.

Portaliso. **A História do Home Office.** Portaliso, [s.d.]. Disponível em: https://homeoffice.portaliso.com/historia-do-home-office/. Acesso em: 28 fev. 2022.

Portaliso. **Como surgiu o Home Office?** Portaliso, [s.d.]. Disponível em: https://homeoffice.portaliso.com/como-surgiu-o-home-office/. Acesso em: 12 mar. 2022.

Positivo Tecnologia**. 6 golpes de engenharia social para ficar de olho**. Positivo Tecnologia, 2018. Disponível em: https://www.meupositivo.com.br/panoramapositivo/golpes-de-engenharia-social/ Acesso em: 5 mai. 2022.

Sebrae. **O que é LGPD?** Sebrae, [s.d.]. Disponível em: https://www.sebrae.com.br/sites/PortalSebrae/canais_adicionais/conheca_lgpd. Acesso em:

2 set. 2022.

TCHILIAN, Felipe**. Engenharia Social: O que é, tipos de ataque, técnicas e como se proteger**. Clear Sale, [s.d.]. Disponível em: https://blogbr.clear.sale/engenharia-social-o-que-e-e-como-se-proteger. Acesso em: 25 abr. 2022.

Tree TI. **Os Desafios da Cibersegurança no Home Office**. Tree TI, 2021. Disponível em: https://treeti.com.br/ciberseguranca-home-office/. Acesso em: 14 set. 2022.

Value Host. **Backdoor: entenda como funcionam os ataques cibernético nas empresas**. Value Host, 2022. Disponível em: https://www.valuehost.com.br/blog/backdoor/. Acesso em: 05 ago. 2022.