INTERFACE TECNOLÓGICA

ESTRATÉGIAS DE DEFESA CONTRA ENGENHARIA SOCIAL EM AMBIENTES DE TRABALHO *HOME OFFICE*

DEFENSE STRATEGIES AGAINST SOCIAL ENGINEERING IN HOME OFFICE WORK ENVIRONMENTS

Ronaldo Rodrigues Martins – ronaldo.martins@fatec.sp.gov.br
Faculdade de Tecnologia de Catanduva – Catanduva – São Paulo – Brasil

João Vitor Fonseca Duarte Silva – joao.silva364@fatec.sp.gov.br
Faculdade de Tecnologia de Catanduva – Catanduva – São Paulo – Brasil Nome

Eduardo Barros Petine de Oliveira – eduardo.oliveira90@fatec.sp.gov.br
Faculdade de Tecnologia de Catanduva – Catanduva – São Paulo – Brasil

DOI: 10.31510/infa.v18i2.1329
Data de submissão: 15/09/2021
Data do aceite: 03/11/2021
Data da publicação: 30/12/2021

RESUMO

Ações defensivas de segurança da informação no ambiente corporativo envolvem pessoas, recursos físicos e tecnológicos. Neste sentido, além de tecnologias e ferramentas, devem ser adotadas políticas e procedimentos que orientem os colaboradores das organizações em suas tarefas diárias de trabalho. Paralelo ao cenário de segurança, a pandemia causada pelo vírus SARS-CoV-2 iniciada no ano de 2020, forçou diversas organizações em todo o mundo a adotar regimes de trabalho em *home office.* Logo essa situação tornou sistemas de informação e a comunicação entre colaboradores mais vulneráveis a ataques de engenharia social devido as pessoas estarem fora do perímetro físico das organizações. Em suma, uma política de segurança da informação atualizada e compartilhada entre os colaboradores das organizações são essenciais para diminuir as chances de sofrer ataques cibernéticos. Diante do contexto supracitado, este artigo tem como objetivo apresentar um panorama das empresas da cidade de Catanduva (São Paulo) que adotaram regime de trabalho *home office* e o conhecimento que seus colaboradores possuem em relação à política de segurança da informação vigente em seus ambientes de trabalho. Neste sentido, acreditamos que os resultados deste trabalho possam orientar gestores de tecnologia da informação na condução de suas políticas de segurança e fomentar futuros trabalhos acadêmicos relacionados a engenharia social.

Palavras-chave: Engenharia Social. Segurança da Informação. *Home Office*

ABSTRACT

Defensive information security actions in the corporate environment involve people, physical and technological resources. In this sense, in addition to technologies and tools, policies and procedures must be adopted to guide employees of organizations in their daily work tasks. Parallel to the security scenario, the pandemic caused by the SARS-CoV-2 virus that started in

INTERFACE TECNOLÓGICA

the year 2020, forced several organizations around the world to adopt home office work regimes. Soon this situation made information systems and communication between employees more vulnerable to social engineering attacks because people are outside the physical perimeter of organizations. In short, an updated information security policy shared among the employees of organizations is essential to reduce the chances of suffering cyber-attacks. Given the context, this article aims to present an overview of companies in the city of Catanduva (São Paulo) that have adopted a home office work regime and the knowledge that their employees have in relation to the information security policy in force in their environments. Work. In this sense, we believe that the results of this work can guide information technology managers in conducting their security policies and foster future academic work related to social engineering.

Keywords: Social Engineering. Information Security. Home Office

INTRODUÇÃO

Na última década, corporações em todo o mundo aumentaram a adoção do formato de trabalho *home office* entre seus colaboradores. Logo a evolução das tecnologias de comunicação tem contribuído para este cenário, como aumento significativo na velocidade e queda dos preços de serviços de internet banda larga, amadurecimento das tecnologias de criptografia e o surgimento de novas aplicações de videoconferência. Corroborando com essa tendência, entre os anos de 2019 e 2020, com o surgimento abrupto de uma pandemia causada pelo vírus SARS-CoV-2, organizações foram obrigadas a adotar regimes de trabalho em formato *home office.* Deste modo, as mesmas se adaptaram à nova realidade tecnológica e medidas de segurança da informação precisaram ser repensadas para ambientes remotos.

Em ambientes corporativos, o universo da segurança da informação está compreendido em ambientes físicos e virtuais, além de procedimentos e políticas de segurança que devem nortear as ações dos colaboradores das organizações. Neste contexto, de acordo com Marcelo e Pereira (2005), a falta de procedimentos e políticas de segurança podem facilitar ações de engenheiros sociais, que exploram comportamentos sociais dos usuários alvos, como vaidade, humildade e egocentrismo para obter dados confidenciais. Logo, a flexibilidade proporcionada pelo trabalho em ambiente *home office* pode corroborar com este tipo de ameaça.

Dentro do universo de vulnerabilidades de segurança, as técnicas de engenharia social quando aplicadas fora do ambiente organizacional, exigem maior esforço das equipes responsáveis pela segurança da informação. No entanto, mesmo que sejam adotadas as tecnologias mais recentes de defesa para ambientes físicos e virtuais, ainda assim é possível sofrer ataques bem-sucedido por meio de ações maliciosas de dia zero (do inglês, *zero day*). Neste sentido, ações de dia zero ocorrem por ataques ou softwares maliciosos desconhecidos

que ainda não possuem ações defensivas definida na academia ou indústria, sendo assim, os procedimentos especificados na política de segurança da informação a última barreira de defesa.

Este artigo tem como objetivo central apresentar um panorama sobre a gestão e compartilhamento de políticas de segurança da informação entre os colaboradores das organizações situadas na cidade de Catanduva S.P.

1. FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta conceitos e definições sobre segurança da informação e engenharia social, além de uma breve introdução sobre conceitos de trabalho em formato *home office* e a pandemia causada pelo vírus Sars-CoV-2. Os assuntos abordados nessa seção são importantes para a compreensão das seções seguintes.

1.1 Pandemia e o modelo de trabalho home office

De acordo com o Instituto Butantan (2021), uma enfermidade que se dissemina em várias regiões do mundo, afetando vários países ou continentes, pode ser considerada uma pandemia.

Os primeiros casos registrados da doença Covid-19, de acordo a WHO (2021), foram comunicados entre dezembro de 2019 e no início de 2020. Esses casos tinham ligação direta com o Mercado Grossista de Frutos do Mar de *Huanan*, situado na cidade de *Wuhan* (China). A maioria dos primeiros pacientes eram proprietários de barracas, funcionários do mercado ou visitantes regulares. Amostras ambientais retiradas desse mercado em dezembro de 2019 testaram positivo para o vírus SARS-CoV-2, sugerindo que o mercado de *Wuhan* tenha sido a origem do surto. Ainda segundo WHO (2021), o vírus pode ter sido introduzido na população através da comercialização de algum animal ou ser humano infectado.

Com a rápida e agressiva disseminação do vírus SARS-CoV-2 por diversos países do mundo, muitos governos decretaram estado de *lockdown* na tentativa diminuir a velocidade de contágio do vírus. Deste modo, foram implantados regime de trabalho *home office* para evitar que suas atividades ficassem paralisadas. De acordo com Froehlich (2020), o regime *home office* é um modo de trabalho flexível, que por meio de tecnologias de informação e comunicação permitem que colaboradores desempenhem suas tarefas em locais fora do domínio físico da organização.

1.2 Segurança da Informação

Alcançar segurança integral em sistemas de informações deve envolver segurança física e tecnológica, e, políticas e procedimentos. Neste sentido, a segurança física envolve

limitação de acesso aos equipamentos, câmeras de monitoramento e sistemas biométricos para permitir o acesso aos dispositivos de tecnologia da informação apenas por pessoas autorizadas. A segurança tecnológica envolve mecanismos de proteção para aplicações, sistemas operacionais e redes de comunicação, como por exemplo sistemas de firewall e proteção contra *spams* e *malwares* (do inglês, *Malicious Software).* E finalmente as políticas e procedimentos são direcionados as pessoas que lidam com recursos de tecnologia da informação. Logo, os colaboradores de uma organização precisam conhecer as políticas e procedimentos de acesso a sites, e-mails, criação de senhas, compartilhamento de recursos, entre outros (DASWANI *et. al*., 2007; SALEEM; HAMMOUDEH, 2018).

De acordo com Peixoto (2006), a segurança da informação deve atender a três pilares para alcançar segurança plena. O primeiro pilar está relacionado a confidencialidade que garante que dados transmitidos por meio de redes de comunicação (em trânsito) ou armazenados em um repositório (em repouso) não sejam acessadas por agentes não autorizados. O segundo pilar trata da integridade de dados em trânsito ou repouso, garantindo que os dados não sejam modificados sem autorização. E o último pilar está relacionado a disponibilidade dos dados, ou seja, é necessário garantir que os dados estejam disponíveis de modo confiável e íntegro.

Com o surgimento da Covid 19 e a implantação de trabalho em regime *home office* por organizações de todo o mundo, tornou o ambiente dos colaboradores mais vulneráveis, sendo que parte da segurança lógica e física ficaram fora do alcance das organizações. Logo, políticas e procedimentos precisam ser revisadas para acompanhar o novo modelo de trabalho.

1.3 Engenharia Social

De acordo com Xiangyu, Qiuyang e Chandel (2017), ataques de engenharia social exploram técnicas de persuasão e trapaça que fazem com que usuários disponibilizem informações sigilosas a pessoas mal-intencionadas. Neste sentido, os ataques de engenharia social podem ser classificados em: (i) **ataques diretos**, que são caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas, mensagens ou pessoalmente; e (ii) **ataques indiretos**, sendo que esses ataques contam com o auxílio de *malwares* ou ferramentas, como por exemplo, vírus, cavalos de troia, sites e/ou e-mails falsos (ALLEN, 2001; PEIXOTO, 2006).

De acordo com Allen (2001), um ataque de engenharia social ocorre por meio de quatro fases, são elas: **Fase 1 (reunir informações)**, nesta fase, informações são coletadas a respeito do alvo almejado, onde busca-se construir um cenário sobre a organização e/ou as

pessoas envolvidas. Algumas das informações mais comuns que podem ser coletadas são: números de telefone, datas de nascimento, informações internas sobre processos da organização, entre outras; **Fase 2 (desenvolver um relacionamento),** de posse das informações colhidas na Fase 1, o engenheiro social busca estabelecer contato com o alvo a fim de traçar uma estratégia de ataque; **Fase 3 (exploração)**, após o estabelecimento de confiança entre o engenheiro social e o alvo, informações sigilosas podem ser reveladas, como senhas, contas, endereços, entre outros; e por fim **Fase 4 (execução),** ataques ou ações maliciosas são consumados e o ciclo de ataque é finalizado.

A ações de engenharia social podem ser aplicadas individualmente ou em conjunto com outras técnicas maliciosos. Neste sentido, alguns ataques iniciam com técnicas de engenharia social para obter dados sigilosos para que em seguida outros métodos sejam utilizados com base nas informações obtidas (PEIXOTO, 2006).

A seguir são apresentadas definições sobre algumas das técnicas de engenharia social mais recorrentes que estão contidas na "Cartilha de Segurança para Internet" no qual é produzida pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) (CERT, 2012).

Furto de identidade. Por meio da criação de contas de e-mail ou perfis de rede social falsas, alteração de campos de e-mail e clonagem de cartões de crédito, um golpista pode se passar por outra pessoa, enviando mensagens ou praticando ações para obter algum tipo de vantagem ou informação sigilosa.

Fraude de antecipação de recursos. O usuário é induzido a antecipar algum tipo de recurso como dinheiro ou informações confidenciais como promessa de recebimento de futura vantagem. Esta fraude pode ser executada por meio de sites, e-mails e aplicativos falsos.

Phishing. O golpista tenta obter vantagens ou informações sigilosas por meio de mensagens eletrônicas que chamam atenção por conter informações sobre instituições conhecidas, mensagens curiosas, cômicas, ameaças de multa ou cancelamento de serviços.

Pharming. Esta técnica é semelhante ao *phishing*, contudo ocorre inicialmente a infecção do sistema de DNS (do inglês, *Domain Name System*) da organização. Portanto quando o usuário busca por um serviço ou site, ocorre o redirecionamento para um endereço falso.

Boatos. Por meio de uma mensagem alarmante e geralmente falsa relacionado a celebridades ou organizações relevantes, *malwares* podem ser distribuídos. Além disso, serviços de rede como e-mail ou web podem ter sua performance comprometida devido ao grande volume de acessos a serviços.

A fim de quebrar a confidencialidade interna de dados das organizações, podem ser utilizados ações de engenharia social de contato direto e indireto com os colaboradores. As ações de contato direto são classificadas em: (i) **Intimidação**: por meio de ameaças ou ações amedrontadoras, colaboradores podem quebrar a confidencialidade de dados. O engenheiro social pode se passar por uma autoridade por exemplo; (ii) **Persuasão**: através de ações persuasivas que iludam os colaboradores, como um ganho de lucro por exemplo, pode revelar informações sigilosas; (iii) **Insinuação**: os invasores constroem relacionamentos de confiança com os colaboradores para então obter dados sigilosos; e (iv) **Assistência**: por meio de abordagens semi-coercitivas, os invasores negociam as informações desejadas. A seguir são apresentadas ações de contato indireto com os colaboradores para obter dados sigilosos: (a) **Ameaças online**: por meio de mensagens eletrônicas trocadas entre os colaboradores através de canais corporativos, como por exemplo e-mail, mensagem instantânea e páginas web, os invasores obtém informações sigilosas; (b) **Ameaças baseadas em telefone**: por meio de ligações telefônicas, agentes maliciosos podem obter informações sigilosas; e (c) **Ameaças baseadas em resíduos**: informações relevantes como identificação e informações de usuários, telefone da empresa ou membros da organizações podem ser descartados como lixo, e a partir dessas informações os invasores podem se disfarçar ou criar relacionamentos com colaboradores da organização.

Para mitigar as ameaças de engenharia social, de acordo com Saleem e Hammoudeh (2018), políticas e procedimentos organizacionais devem ser definidos e compartilhados entre os colaboradores de uma organização. Neste sentido, é possível que mecanismos de segurança físico e tecnológico falhem devido ao crescente aumento de novas ações maliciosas. Portanto, em situações que estes mecanismos falhem, as políticas e procedimentos organizacionais podem ser a última barreira de defesa em uma organização.

A política de segurança da informação (PSI) é a ferramenta fundamental para formalizar procedimentos e políticas de segurança em uma organização. Por meio da PSI são definidos diretrizes e limites para os controles que serão implantados, portanto, neste documento constam instruções e procedimentos que os colaboradores devem conhecer e praticar, além de uma hierarquia definindo quais informações cada usuário pode acessar, assim como ações que devem ser seguidas em situações emergências. Em suma, de acordo com a ABNT ISO/IEC 27002, a PSI deve conter uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação, uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação.

É de responsabilidade das organizações garantir ampla divulgação e treinamento da PSI aos colaboradores (FONTES, 2012). Entretanto, de acordo com Saleem e Hammoudeh (2018), ao participar de uma sessão de treinamento, os colaboradores tendem a esquecer 50% do conteúdo após uma hora, 70% em 24 horas e 90% em uma semana. Neste sentido, os treinamentos relacionados às políticas e procedimentos de segurança devem fazer parte de um programa de conscientização e treinamento continuado (ALDAWOOD; SKINNER, 2019).

Segundo Georgiadou, Mouzakitis e Askounis (2021), durante o período de pandemia causada pela SARS-CoV-2, as empresas que apresentaram os melhores resultados de segurança, implementaram VPN (do inglês, *Virtual Private Network*) como meio de comunicação. Além disso, foram adotadas boas práticas de segurança, a sabe são: proteger os e-mails utilizando senha forte; ativar autenticação de dois fatores nos e-mails; fazer backups frequentemente de dados importantes; proteger smartfones e tablets com senhas na tela de bloqueio e utilizar gerenciador de senhas (FURNELL;SHAH, 2020).

2. PROCEDIMENTOS METODOLÓGICOS

Este trabalho tem como objetivo buscar entender a relação entre colaboradores e política de segurança da informação, durante o período de *home office* em decorrência da pandemia causada pelo vírus SARS-CoV-2, em empresas da cidade de Catanduva (São Paulo).

Em uma primeira etapa foi realizado uma pesquisa bibliográfica (Seção 1) sobre os principais conceitos relacionados a ataques e vulnerabilidades de engenharia social, meios de defesas, além de um histórico sobre a pandemia causadora pelo vírus SARS-CoV-2. Na sequência, por meio de uma pesquisa de campo através de questionário on-line (Seção 2) foram levantados dados sobre a gestão e compartilhamento das políticas de segurança da informação entre os colaboradores das empresas. Na sequência são apresentados os resultados coletados (Seção 3), e por fim são apresentadas as considerações finais do estudo (Seção 4).

2.1 Questões de Pesquisa

O Quadro 1 apresenta as questões de pesquisa que foram respondidas por colaboradores das organizações selecionadas para este estudo, sendo que as questões foram disponibilizadas por meio da plataforma Web. Cabe ressaltar que os colaboradores participantes não fazem parte da equipe de segurança da informação ou gestora da política de segurança da informação. Neste contexto, o requisito principal para a participação da pesquisa é que o colaborador tenha lidado diretamente com algum sistema de informação em regime de trabalho

home office no período de pandemia. Portanto, o principal objetivo das questões é compreender o nível de conhecimento dos colaboradores a respeito da política de segurança da informação adotado na organização em que trabalham e qual a frequência que recebem treinamentos sobre as políticas.

Quadro 1 - Questões de Colaborador

Questão	**Alternativas**
1 - Você é colaborador a quanto tempo da organização	a) A pelo menos 6 meses b) A pelo menos 1 ano c) A pelo menos 2 anos d) A mais de 2 anos
2 - A organização possui uma política de segurança da informação que defina os procedimentos que os colaboradores devam seguir, como sites que não devem ser acessados, identificar e-mails maliciosos, identificar e reagir a ações hackers, identificar e reagir a lições telefônicas falsas, softwares que podem ou não ser instalados, entre outros?	a) Conheço completamente a política de segurança da organização. b) Conheço a política de segurança, porém não me lembro de todos os pontos claramente. c) Não existe uma política de segurança formal, mas existe uma cultura de segurança da informação entre os colaboradores d) Desconheço uma política ou cultura de segurança da informação na organização
3 - Você já recebeu ou recebe treinamentos periódicos sobre segurança da informação?	a) Recebi um treinamento. b) Recebo treinamentos esporádicos. c) Recebo treinamento quinzenalmente. d) Recebo treinamento mensalmente. e) Recebo treinamento bimestrais. f) Recebo treinamento Trimestrais. g) Recebo treinamento semestralmente h) Recebo treinamento anualmente. i) Nunca recebi treinamento a respeito de política de segurança da informação.
4 - Você trabalhou em regime home office em decorrência da pandemia (Covid-19) causada pelo vírus Sars-CoV-2?	a) Sim b) Não
4.1 - Neste período você utilizou computador fornecido pela empresa ou computador pessoal?	a) Computador Pessoal. b) Computador da Empresa. c) Computador pessoal e da empresa.

Fonte: Autoria própria

3. APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

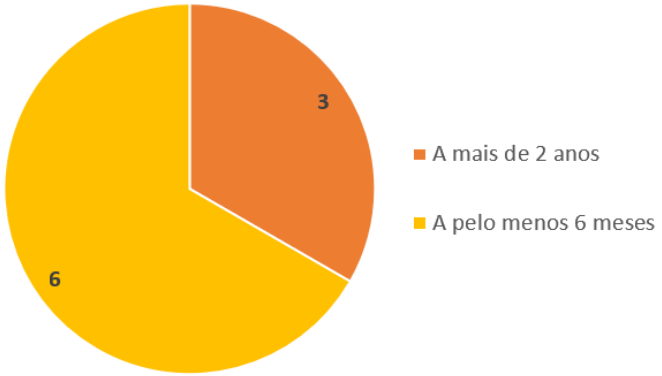
Nesta seção, são apresentados os dados coletados a partir das questões apresentadas no Quadros 1. O questionário foi respondido por 9 colaboradores de 6 diferentes organizações da cidade de Catanduva (São Paulo). Por tratarem de questões sensíveis relacionadas à segurança da informação, as organizações e identidades dos colaboradores participantes do questionário não serão divulgados neste trabalho. Das 6 organizações participantes, 2 são do ramo de tecnologia da informação, 2 do ramo educacional, 1 do ramo varejista e 1 do ramo industrial.

3.1 Questão 1

Esta questão apresenta a quanto tempo cada colaborador possui vínculo com a organização. De acordo com a Figura 1, 6 dos participantes possuem vínculo a pelo menos 6 meses e 3 possuem vínculo a pelo menos 2 anos.

O tempo de vínculo do colaborador com a empresa é importante para compreender a questão 2, que trata a respeito da periodicidade em que os colaboradores recebem treinamento referente a políticas de segurança da informação.

Figura 1 - Colaboradores (Questão 1)



Fonte: Autoria própria

3.2 Questão 2

Esta questão apresenta o nível de conhecimento sobre a política de segurança da informação da organização para cada participante. De acordo com a Figura 2, 7 dos participantes conhecem a política de segurança, porém não se lembram de todos os pontos claramente e 2 conhecem claramente a política de segurança da organização. Logo os dados

apontam que as organizações participantes possuem alguma política de segurança da informação, além disso, as políticas são compartilhadas com seus colaboradores.

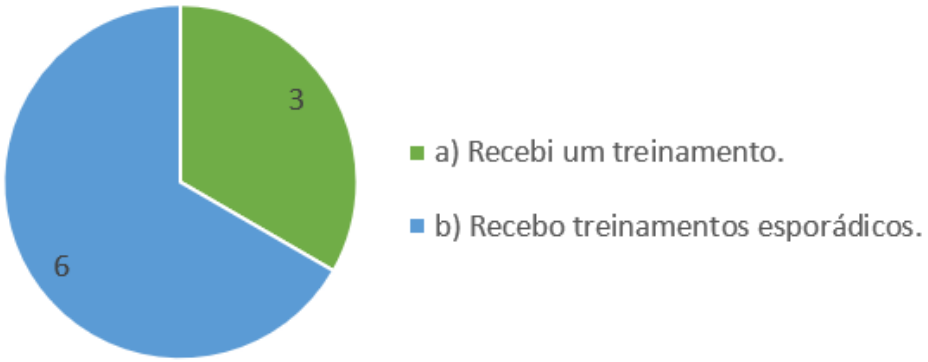
Figura 2 - Colaboradores (Questão 2)

Fonte: Autoria própria

3.3 Questão 3

A questão 3 apresenta a periodicidade que os colaboradores recebem treinamento sobre políticas de segurança. Conforme ilustrado pela Figura 3, 6 dos participantes responderam que recebem treinamentos esporádicos e 3 responderam que receberam apenas 1 treinamento. Os dados evidenciam que as empresas participantes da pesquisa não mantem um programa periódico de conscientização de segurança da informação entre seus colaboradores.

Figura 3 - Colaboradores (Questões 3 e 3.1)



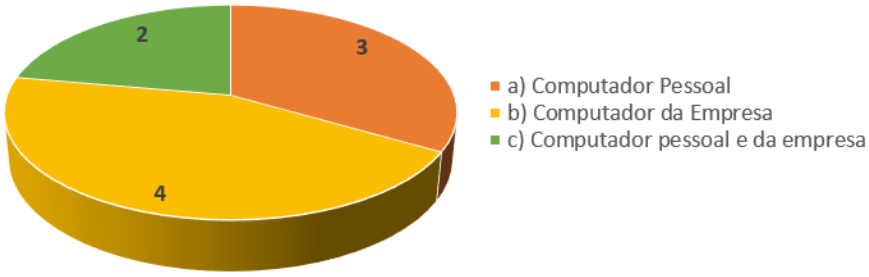
Fonte: Autoria própria

3.4 Questões 4 e 4.1

A questão 4 aponta se os colaboradores adotaram regime de trabalho *home office* em decorrência da pandemia causada pelo vírus SARS-CoV-2. Neste ponto, os participantes foram unanimes em apontar que adotaram regime de trabalho *home office* em algum momento durante a pandemia. Neste período, de acordo com a Figura 4, 4 dos colaboradores utilizaram

computadores fornecidos pela empresa, 2 utilizaram computadores fornecidos pela empresa e computador pessoal e 3 utilizaram apenas computadores pessoais.

Figura 4 - Colaboradores (Questões 4 e 4.1)



Fonte: Autoria própria

Os dados coletados apontam que metade dos colaboradores utilizam computadores pessoais durante o trabalho em regime *home office*. Portanto, isso demonstra que ferramentas de segurança adotadas pelas organizações podem não ter sido suficientes para manter dados confidenciais, evidenciando possíveis vulnerabilidades ao acesso a dados pelos colaboradores. Neste sentido, as políticas de segurança da informação devem ser periodicamente compartilhadas com os colaboradores por meio de treinamentos e revisões como tentativa de manter uma última barreira de segurança, que são os próprios comportamentos dos colaboradores.

4. CONSIDERAÇÕES FINAIS

Muitas organizações possuem mecanismos voltados a segurança física e digital, mas acabam negligenciando o elo mais fraco da segurança da informação, as pessoas. Logo, procedimentos e políticas de segurança devem ser adotados para nortear os colaboradores em suas tarefas diárias. Neste sentido é necessário que as organizações tenham programas de conscientização periódicos junto aos colaboradores.

De acordo com as amostras de dados apresentadas nesse trabalho, foi possível reunir evidências que organizações da região da cidade de Catanduva (São Paulo), são carentes de políticas formais de segurança da informação. Onde a cultura de segurança da informação existente não é reforçada junto aos colaboradores por meio de ações periódicas de conscientização. Além disso, os participantes da pesquisa informaram que não houve alterações nas políticas de segurança da informação no período de regime de trabalho *home office*. O que pode evidenciar que as organizações ficaram mais vulneráveis a ataques de engenharia social no período de pandemia.

Diante do resultado da pesquisa, é recomendável que as organizações criem políticas de segurança da informação formais para futuras adoções de regimes de trabalho *home office.* Neste sentido, é importante que as organizações mantenham com seus colaboradores, programas de conscientização periódicos sobre suas políticas de segurança da informação. Além disso, acreditamos que este artigo possa fomentar novas pesquisas acadêmicas nas áreas de segurança da informação, engenharia social e políticas e procedimentos de segurança da informação.

REFERÊNCIAS

ALDAWOOD, H; SKINNER, G. **Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering**, 2019. Cybersecurity and Cyberforensics Conference (CCC), 2019, pp. 111-117. Disponível em http://tiny.cc/x35juz. Acessado em 01/09/2021.

ALLEN, Malcolm. **Social Engineering**: A Means to Violate a Computer System. 2001. Disponível em http://tiny.cc/w35juz. Acessado em 19 agosto de 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2013**, 2013. Disponível em https://www.abntcatalogo.com.br. Acessado em 09/11/2021.

CERT. **Cartilha de Segurança para Internet**. 2012. Disponível em https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acessado em 19 agosto de 2021.

DASWANI, N; KERN, C; KESAVAN, A**. Foundations of Security: What Every Programmer Needs to Know**, 2007. Springer-Verlag New York.

FONTES, E. **Políticas e Normas para a Segurança da Informação.** Rio de Janeiro: Brasport, 2012.

FROEHLICH, C. **Benefícios e Desafios do Home Office em Empresas de Tecnologia da Informação**, 2020. Disponível em http://tiny.cc/t35juz. Acessado em 20/08/2021.

FURNELL, S.; SHAH, J.N. **Home working and cyber security – an outbreak of unpreparedness?. Computer Fraud & Security**, 2020, pp 6–12. Disponível em: http://tiny.cc/9j9luz. Acessado em 08/11/2021.

GEORGIADOU, A.; MOUZAKITIS, S.; ASKOUNIS, D. **Working from home during COVID-19 crisis: a cyber security culture assessment survey**. Security Journal, 2021. Disponível em: https://doi.org/10.1057/s41284-021-00286-2. Acessado em 08/11/2021.

HADNAGY, C. **Social Engineering: The Science of Human Hacking**. Indianapolis: WileyPublishingInc, 2011.

INSTITUTO BUTANTAN. **Entenda o que é uma pandemia e as diferenças entre surto, epidemia e endemia,** 2021. Disponível em http://tiny.cc/o35juz. Acessado em 20/08/2021.

MARCELO A.; Pereira, M. **Engenharia Social: hackeando pessoas.** Brasport, 2005.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

SALEEM, J.; HAMMOUDEH, M. **Defense Methods Against Social Engineering Attacks**, 2018. In: Daimi K. (eds) Computer and Network Security Essentials. Springer, Cham.

WHO. **Origins of the SARS-CoV-2 virus**, 2021. Disponível em http://tiny.cc/k35juz. Acessado em 20/08/2021.

XIANGYU, L; QIUYANG, L; CHANDEL, S. **Social engineering and insider threats**. *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2017, pp. 25-34, doi: 10.1109/CyberC.2017.91. Disponível em http://tiny.cc/i35juz. Acessado em 01/09/2021.