FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Gabriele Arbertavicius

Mario Octavio Cordeiro Carmesini

O aumento de casos de engenharia social durante a pandemia de COVID-19

Americana, SP
2022

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Gabriele Arbertavicius

Mario Octavio Cordeiro Carmesini

O aumento de casos de engenharia social durante a pandemia de COVID-19

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Esp. Bruno Henrique de Paula Ferreira.

Área de concentração: Conceitos de engenharia social.

Americana, SP
2022

Gabriele Arbertavicius
Mario Octavio Cordeiro Carmesini

O aumento de casos de engenharia social durante a pandemia de COVID-19

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: Conceitos de engenharia social.

Americana, 03 de dezembro de 2022

Banca Examinadora:

Bruno Henrique De Paula Ferreira (Presidente)
Especialista
Fatec Americana

Carlos Henrique Sarro (Membro)
Mestre
Fatec Americana

Wellington Aires da Cruz Pereira (Membro)
Mestre
Fatec Americana

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

O aumento de casos de engenharia social durante a pandemia de COVID-19

Gabriele Arbertavicius

Mario Octavio Cordeiro Carmesini

gabriele.arbertavicius@fatec.sp.gov.br

mario.carmesini@fatec.sp.gov.br

Abstract. *A lot of things have changed in the last few months. Due to the current global condition in which we find ourselves, the digital scenario has migrated from large companies and offices into our homes, whether in the form of a home office, online classes or just more free time, we had to adapt in an unprecedented way to be exposed to a river of information and mischief, all the time.*

Resumo. *Muitas coisas mudaram nos últimos meses. Devido a atual condição mundial na qual nos encontramos, o cenário digital migrou das grandes empresas, companhias e escritórios para dentro de nossas casas, seja em forma de home office, de aulas online ou apenas maior tempo livre, tivemos que nos adaptar de forma inédita a estarmos expostos à um rio de informações e possíveis golpes, o tempo todo.*

1. Introdução

Ao longo da última década, empresas em todo o mundo aumentaram a aceitação do formato home office entre seus funcionários. Portanto, o desenvolvimento das tecnologias de comunicação tem contribuído para esse cenário, como o aumento significativo da velocidade e a diminuição do preço dos serviços de internet banda larga, o amadurecimento das tecnologias de criptografia e o surgimento de novos aplicativos de videoconferência (ROCHA, 2020).

Esta tendência foi sustentada entre 2019 e 2020 pelo início súbito de uma pandemia causada pelo vírus SARS-CoV-2, as empresas foram obrigadas a adotar sistemas de trabalho no formato home office. O atual cenário de pandemia, diante da turbulência sanitária e econômica, exige maior uso e aplicação das Tecnologias de Informação e Comunicação (TIC), ao lado de ferramentas, ambientes e práticas sociais nas mais diversas esferas da vida humana (NAGLI, 2020).

Dessa forma, eles se adaptaram à nova realidade tecnológica e as medidas de segurança da informação tiveram que ser reconsideradas para ambientes remotos. Um dos fenômenos emergentes da pandemia do COVID-19 está relacionado aos golpes digitais que, utilizando dados pessoais de brasileiros e utilizando técnicas de persuasão, induzem as vítimas a confiar e cometer erros, como o fornecimento de seus dados bancários ou a realização de transações financeiras em nome do golpista (JÚNIOR et al., 2020).

As mais diversas atividades, além das financeiras e econômicas, são alvo desses golpes, como as relacionadas à comunicação por meio de aplicativos de mensagens instantâneas, comércio eletrônico, instalação de aplicativos, entre outros. No entanto, as atividades que envolvem pagamentos, recebimentos, financiamentos e outras transações financeiras merecem destaque por seu grande potencial de prejudicar suas vítimas e aumentar a crise econômica no país e no mundo (NAGLI, 2020).

No universo das vulnerabilidades, as técnicas de engenharia social, quando aplicadas fora do ambiente corporativo, exigem maior esforço das equipes de segurança da informação. No entanto, mesmo quando as tecnologias de defesa mais recentes são implantadas em ambientes físicos e virtuais, ainda é possível sustentar ataques bem-sucedidos por meio de ações maliciosas de dia zero (JUNIOR et al., 2020).

Para que esse contexto possa ser melhor entendido, pode-se recorrer à segurança da informação, uma disciplina da área de informática que deixou de se referir apenas às grandes empresas e se popularizou com a transformação digital da sociedade de pequeno e médio porte. A ascensão das ameaças digitais tem levantado questões como violações de privacidade e capitalização de dados, entre outras (BIONI et al, 2020; KSHETRI, 2020; MODESTO, EHRHARDT JUNIOR, 2020; SILVEIRA, 2017).

Assim sendo, com o ambiente tendo mudado em grande parte para dentro de nossas casas, aumenta-se o uso de internet e redes sociais, que, apesar de ser uma boa forma de manter contato com os amigos e familiares, são também uma fonte de ansiedade pelo grande fluxo de informações, nem sempre verídicas, e, além de causar uma grande dependência aos seus usuários, ainda maior do que isso, há o problema que enfrentamos em casos de engenharia social, já que, estando o tempo todo em casa, ficamos ainda mais suscetíveis a esse tipo de ataque. Devido ao crescente número de fraudes digitais, a segurança da informação está se tornando uma preocupação cada vez mais popular.

Dessa maneira, o objetivo deste trabalho é conhecer mais sobre o conceito de engenharia social, e descrever sobre o aumento do número de casos desse método de ataque durante a pandemia da covid-19. Como objetivos específicos o trabalho possui: descrever engenharia social e seus diversos tipos, examinar o contexto e questões relacionadas à pandemia e apresentá-los sob a ótica da engenharia social e mostrar quais são as principais formas e ferramentas utilizadas para que as pessoas e empresas se defendam desses ataques.

O método utilizado para a realização deste trabalho foi a revisão de literatura. Foram realizadas pesquisas em bases de dados como Lilacs, Scielo, Capes e Google Acadêmico, de artigos publicados nos idiomas português e inglês

O trabalho está estruturado em 3 capítulos, sendo a introdução, o desenvolvimento e as considerações finais. Como observado neste tópico, a introdução realiza uma contextualização atual do tema, justifica a realização do trabalho, além de apresentar a metodologia utilizada e os objetivos do trabalho. O segundo capítulo desenvolve conceitos de engenharia social, relata seu aumento durante a pandemia da covid-19 e menciona maneiras de proteção a esses ataques. Por fim, o último capítulo, realiza uma análise da visão geral dos autores desenvolvidos no referencial teórico deste trabalho.

2. Revisão bibliográfica

2.1. Internet

A Internet surgiu no contexto da Guerra Fria protagonizada pela até então União Soviética e os Estados Unidos. Durante a época, muitas tecnologias surgiram e/ou foram aperfeiçoadas com o intuito de facilitar a troca de informações de forma segura a fim de

facilitar estratégias. O protótipo da primeira rede de internet chamava-se ARPAnet, em inglês, *Advanced Research Projects Agency Network*. Já a Internet como conhecemos hoje surgiu na década de 90, com o desenvolvimento da *World Wide Web*, a nossa Rede Mundial de Computadores.

No Brasil, até 1995, o acesso à Internet era restrito à estudantes, professores e instituições de pesquisa, além de instituições governamentais e privadas. Em maio deste mesmo ano, o Governo Federal editou em uma Nota Conjunta do Ministério das Comunicações e o Ministério da Ciência e Tecnologia o que era a Internet:

> A Internet é um conjunto de redes interligadas, de abrangência mundial. Através da Internet estão disponíveis serviços como correio eletrônico, transferência de arquivos, acesso remoto a computadores, acesso a bases de dados e diversos tipos de serviços de informação, cobrindo praticamente todas as áreas de interesse da Sociedade (BRASIL, 1995).

Assim, seguindo esse ano, fez-se possível que usuários fora dessas regras pudessem obter acesso à Internet, uma vez que a iniciativa privada começou a fornecer o serviço. Doravante esse momento, o Brasil começa a instalar-se na Internet como é hoje.

2.2. Redes Sociais

Um dos primeiros traços de rede social que pode ser citado é o lançamento do GeoCities, em 1994. O mesmo funcionava como um serviço de blog, onde as pessoas podiam criar suas próprias páginas na web, categorizadas de acordo com sua localização. O GeoCities encerrou seu serviço em 2009.

Seguindo essa fórmula, em 1995, foi fundado por dois estudantes o The Globe. Esse dava a liberdade ao usuário de personalizar sua experiência online ao publicar conteúdos que o interessava e permitir encontrar usuários com interesses em comum.

Contudo, a era que marcou a explosão das redes sociais foram os anos 2000, criando as redes sociais que nos acompanham até hoje, como forma de nos expressar, nos comunicar com amigos e encontrar pessoas inspirações em comum. Em 2002 nasceu o Fotolog, onde postavam-se fotos acompanhadas por legenda de autoria do usuário. O Fotolog chegou a atingir 32 milhões de usuários e existe até hoje. No ano seguinte, surgiram o MySpace e o LinkedIn, considerada como uma rede social para profissionais.

Já em 2004, nasce o Orkut, que tornou-se extremamente popular no Brasil, sendo durante anos a mais usada pelos brasileiros. O Orkut foi revolucionário como rede social, juntando diversas outras redes em uma. Tal qual o Fotolog, era possível postar suas fotos com legendas, além de participar de comunidades e encontrar colegas com os mesmos interesses, encontrar amigos próximos, mandar mensagens, depoimentos e jogar, além de diversas outras funcionalidades. O Orkut entrou em declínio em 2011 e encerrou seu serviço em 2014, após perder uma grande base de usuários para o Facebook, que reunia todas essas funcionalidades e muito mais. Durante essa década, ainda surgiram as redes sociais populares hoje em dia, como o Twitter, Instagram, Pinterest e Reddit.

2.3. Engenharia Social

Engenharia social é um termo usado para descrever um método usado para realizar um ataque, esse método é usado constantemente em muitos campos. Segundo Mann (2011) e Thomas (2007), o alvo desse ataque são justamente os humanos, pois os humanos são o elo mais fraco na segurança de uma organização, razão pela qual os ataques de engenharia social estão aumentando no Brasil.

A engenharia social é um método muito eficaz, basicamente se resume a enganar a vítima, criar intimidade, trair sua inocência e confiança, o atacante consegue explorar

diferentes áreas da emoção humana para realizar o ataque, como curiosidade sobre por onde a vítima está entrando o link por curiosidade e inocência, não sabendo que é um link malicioso, muitas vezes em uma empresa, o invasor disca como alvo para um funcionário que tem acesso ao sistema várias ferramentas e métodos para obter informações desta forma pode conceder acesso ao sistema (JÚNIOR et al., 2020).

Nesse sentido, a engenharia social se comporta e se vê como uma ameaça à segurança da informação. A segurança da informação é definida com base em propriedades relacionadas à informação e sistemas informatizados, como confidencialidade, integridade e disponibilidade, que correspondem à proteção das propriedades (ou requisitos) da informação. Outras propriedades como confiabilidade, irreversibilidade, privacidade, autenticidade também podem ser levadas em consideração (DE LUCAS BASTOS et al., 2021).

O ataque de engenharia social também pode ser parte de um ataque maior, onde o invasor deseja obter acesso a um sistema ou organização. Também pode ser um ataque que visa explorar a vítima, apresentando-se na forma de vários golpes e usando várias técnicas como phishing, hoax, spoofing de email e typosquatting (DE LUCAS BASTOS et al., 2021).

Phishing, técnica em que o invasor tenta obter informações confidenciais, como informações financeiras e credenciais de login disfarçadas de terceiros para enganar a vítima. De acordo com Kaspersky (2020), cerca de um em cada oito usuários no Brasil acessou um link para sites maliciosos, o que coloca o Brasil em quinto lugar no ranking mundial de vítimas de phishing.

Hoax ou boato é o uso de mensagens com conteúdo alarmante e linguagem e conteúdo sensacionalistas para enganar e atrair as vítimas, seja para dar vantagem aos golpistas ou para espalhar a mensagem eles mesmos.

O email spoofing consiste em uma técnica que visa adicionar autenticidade às mensagens dos golpistas, alterando o cabeçalho da mensagem para falsificar o remetente e enganar o destinatário, anexos nesses emails podem contar ransomware. Já o typosquatting é a técnica de criar URLs falsos mais semelhantes aos que se deseja falsificar usando erros de ortografia e símbolos. Desta forma, a vítima é redirecionada para um site falso (DE LUCAS BASTOS et al., 2021).

Segundo Xiangyu, Qiuyang e Chandel (2017), os ataques de engenharia social fazem a utilização de alguns métodos e técnicas, além de truques de persuasão que induzem os usuários a fornecer informações confidenciais a indivíduos mal-intencionados.

Dessa forma, os ataques de engenharia social podem ser classificados em: ataques diretos, que são caracterizados pelo contato direto entre o engenheiro social e a vítima por meio de ligações telefônicas, mensagens ou pessoalmente; e ataques indiretos, que são queles que contam com a ajuda de malware ou ferramentas como vírus, trojans, sites falsos e/ou emails (PEIXOTO, 2006).

As ações cometidas pela engenharia social podem ser utilizadas sozinhas ou de maneira conjunta com outras técnicas maliciosas. Dessa maneira, alguns ataques começam com técnicas de engenharia social para obtenção de dados sensíveis, para que outros métodos sejam então utilizados com base nas informações obtidas (PEIXOTO, 2006).

3. Ataques de Engenharia Social durante a Pandemia

De acordo com Mackay (2022), uma pesquisa realizada pela Beaming mostrou

que as empresas do Reino Unido enfrentaram uma tentativa de roubo de dados a cada 47 segundos no ano de 2021. O relatório apontou que o trabalho remoto foi uma oportunidade para ampliar os ataques cibernéticos e que 85% das violações de dados exigiram que um ser humano as iniciasse.

Esse quadro é fomentado pela engenharia social e consiste em uma tática que abrange uma série de atividades que manipulam o comportamento humano. Os cibercriminosos usam a maior quantidade de ferramentas possíveis para atacar os usuários, usando até mesmo truques psicológicos conhecidos para conseguir cliques antes de pensar ou baixar o malware (DE LUCAS BASTOS et al., 2021).

Um relatório recente mostrou que os ataques cibernéticos baseados em Engenharia Social aumentaram 270% em 2021. O mesmo relatório aponta que uma das maneiras de evitar que os engenheiros sociais manipulem os usuários é entendendo como os ataques de engenharia social funcionam (MACKAY, 2022).

Em relação aos ataques mais recentes de Engenharia Social a serem considerados no período da pandemia da covid-19 podem ser citados as ameaças de segurança cibernética. Os cibercriminosos reconhecem que usar funcionários, não funcionários e o ecossistema mais amplo de fornecedores para realizar seus desejos maldosos é uma boa maneira de invadir uma rede segura, fazendo com que estes utilizem chamadas de email recebidas que acabam em um site malicioso (SANTOS, 2020).

Os ataques de engenharia social usam táticas comuns que funcionam repetidamente. Mas os hackers podem variar essas táticas à medida que os eventos se desenrolam. A pandemia de Covid-19 foi um desses eventos. Alguns dos prováveis ataques de engenharia social a serem observados no próximo ano são o *Business Email Compromise* (BEC) e o *Vendor Email Compromise* (VEC) (SANTOS, 2020).

O Relatório de Investigação de Violação de Dados da Verizon (DBIR) de 2021 descobriu que o BEC era a segunda forma mais comum de ataque de engenharia social. BEC e VEC representam a engenharia social em sua forma mais complicada e em camadas.

Os golpistas de BEC usam vigilância para entender seu alvo e criar mensagens de email personalizadas, legítimas, mas falsas. Muitas vezes, um ataque BEC começa com uma conta de comprometida. Isso fornece aos golpistas as informações necessárias para realizar truques sofisticados.

De acordo com Mackay (2022), algumas senhas, como também contas pode ser comprometidas e redirecionadas para permitir que o hacker monitore as operações e comunicações da empresa ou de algum usuário e colete todas as informações necessárias para induzí-los a criar novas contas ou alterar as contas existentes para transferir fundos de empresas ou fundos pessoais para os golpistas de envio.

Segundo Paz e Santos (2021), o *Relatório Business Email Security Landscape Report*, no ano de 2021, forneceu conhecimentos necessários que ajudaram a suavizar o sucesso destes tipos de ataques. Ainda de acordo com este relatório 72% dos inquiridos tinham sofrido um ataque BEC nos últimos 12 meses e quase 50% destes utilizaram uma identidade falsificada apresentada na exibição do nome do email (SANTOS, 2020).

Outro tipo de ataque são os emails de phishing da spear. Estes buscam aquelas pessoas que possuem o poder de movimentar dinheiro. Estas mensagens de correio eletrônico de phishing dirigidas utilizam nomes de empresas (68%), nomes de alvos individuais (66%), e o nome do chefe/gestor (53%) para personalizar o ataque. Uma nova variante do BEC é o *Vendor Email Compromise* (VEC). Esse tipo de BEC se concentra em vendedores para redirecionar fundos. Os ataques VEC usam um efeito em cadeia, com o phishing se espalhando por todo o ecossistema do fornecedor se não for controlado

(PAZ & SANTOS, 2021).

Os ataques VEC são normalmente realizados por criminosos cibernéticos profissionais bem financiados, pois envolvem vigilância e reconhecimento completos para entender seus objetivos o suficiente para serem enganosos e comunicação credível. As técnicas de engenharia social estão no coração do VEC, assim como estão no coração do BEC, a única diferença é que os cibercriminosos estão atacando um ecossistema inteiro (PAZ & SANTOS, 2021).

Tal como acontece com o BEC, o objetivo do golpista VEC é fraudar uma empresa e roubar fundos. O tempo é uma parte importante de um ataque VEC, e a engenharia social é usada para induzir os funcionários a alterar os detalhes de uma fatura no momento certo para evitar suspeitas.

O BEC está entre os muitos tipos de ataques cibernéticos que usam phishing ou spear phishing para iniciar um ataque. Esta técnica é uma das favoritas dos engenheiros sociais e esteve presente em 36% das violações, de acordo com o DBIR. O phishing é a ferramenta definitiva no arsenal dos engenheiros sociais, pois seu conteúdo e contexto podem levar ao controle sobre uma rede corporativa (SANTOS, 2020).

Ainda de acordo com Mackay (2022), estes emails usam uma variedade de truques e gatilhos psicológicos para induzir os destinatários a pensar em um link malicioso para clicar ou email para baixar o anexo infectado. Esses truques incluem spoofing de marcas conhecidas, usando urgência e medo para incentivar cliques e desencadear emoções como *Fear of Missing Out* (FOMO). O phishing geralmente segue os eventos ou tem como alvo os usuários para fins específicos. Os eventos geralmente podem ser um gatilho emocional para um indivíduo. Os golpistas usam essas emoções para fazer com que os usuários sintam que estão perdendo alguma coisa ou que precisam agir com urgência para aproveitar um evento.

Segundo Paz e Santos (2021), durante a pandemia de Covid-19, muitos emails de phishing espelhavam a marca da Organização Mundial da Saúde e brincavam com as preocupações com a saúde dos destinatários de email. Em um determinado momento, durante a pandemia, o Google chegou a bloquear em torno de 17 milhões de emails fraudulentos por dia, com muitos golpistas usando a pandemia para brincar com as emoções e medos das pessoas. Ainda de acordo com o autor, um dos exemplos foi que um único email fraudulento na caixa de entrada de um funcionário de uma empresa, foi capaz de provocar uma violação catastrófica dos dados de vários funcionários da mesma empresa.

O phishing continua a ser usado para iniciar ataques de computador, pois é uma maneira de os cibercriminosos se comunicarem com pessoas que fazem parte de um objetivo corporativo. Usar esse método de comunicação é uma maneira perfeita de manipular socialmente uma pessoa, o que significa que o cibercriminoso não precisa piratear tecnologia do proprietário, em vez disso, eles sequestram todas as informações e tecnologias da pessoa (SANTOS, 2020).

Algo a ser mencionado em relação aos ataques da engenharia social é a falsificação profunda. Ela tem sido o auge destes cibercriminosos e é sabido que as organizações devem esperar que essa tecnologia seja usada para fins catastróficos nos próximos anos. A engenharia social fornece aos hackers maneiras de obter acesso a vários recursos. O fato de esses criminosos operarem em um domínio digital não muda o fato de que o cibercriminoso pode também está observando o comportamento da pessoa que está sofrendo o ataque (GEWEHR, 2020).

Para evitar que os engenheiros sociais manipulem as pessoas, ou uma a rede mais ampla de negócios, por exemplo, é necessário conhecer as formas individuais e a maneira

de atuação desses engenheiros sociais, ou seja, as pessoas precisam ser treinadas para conhecer esses ataques (GEWEHR, 2020).

Dessa forma, pode-se dizer, que possui conhecimento é ter poder, e esse poder precisa ser transferido do cibercriminoso para a empresa ou para a pessoa que está sofrendo o ataque. No caso das empresas, isso será alcançado treinando funcionários e usando sistemas de informação para interceptar tentativas (SANTOS, 2020).

A líder global no quesito em soluções de segurança a ataques cibernéticos, conhecida como Trend Micro, publicou neste ano o relatório Fast Facts que analisa o cenário global de ameaças cibernéticas para o mês de março de 2022, incluindo uma comparação com os meses anteriores. A pesquisa mostrou que o Brasil continua no topo do ranking de ameaças de extorsão por email, incluindo as de natureza sexual, usando endereços IP exclusivos. Outros dois países sul-americanos apareceram na lista dos 10 maiores culpados desse tipo de crime digital, sendo eles Argentina e Peru, como pode ser observado na imagem 1, abaixo (Associação Brasileira das Empresas de Software - ABES, 2022).

Imagem 1. Ranking dos dez principais países culpados de crimes digitais

Fonte: Abes (2022)

Ainda de acordo com o Abes (2022), a tendência de aumento no número de ataques cibernéticos continuou em março do ano de 2022 com um total de 11,2 bilhões de ameaças, das quais 7 bilhões foram bloqueadas, incluindo 124 milhões por email (63% das ameaças detectadas). Em 2021, em plena pandemia, a Trend Micro bloqueou 94,2 bilhões de tentativas de ataques cibernéticos, um aumento de 42% em relação a 2020.

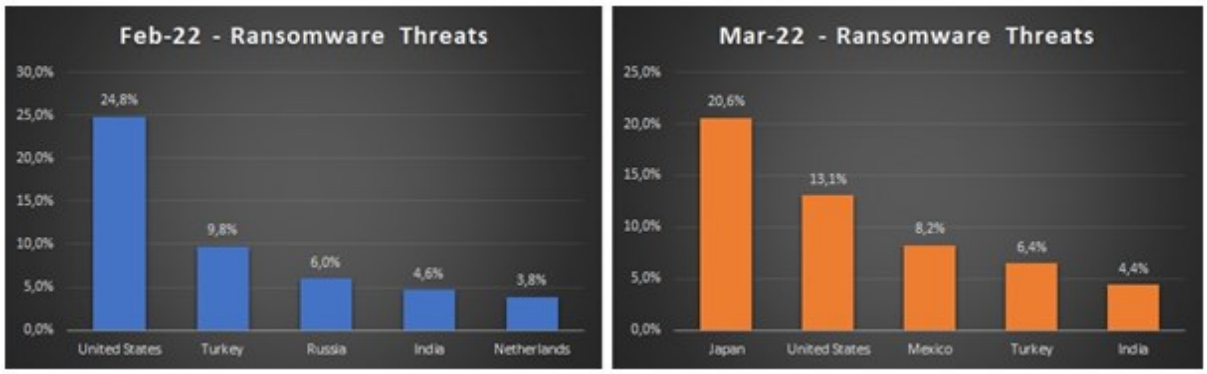
Destes, quase 70 bilhões vieram através de email. Pode ser observado que os Estados Unidos (31,2%) continuam sendo o principal alvo desse tipo de ataque, seguido por China (9,7%) em segundo lugar. O Reino Unido (6,1%) é o terceiro, seguido pelo Japão (5,5%) e Índia (5,1%), (ABES, 2022), como pode ser visto na imagem 2 abaixo.

Imagem 2. Principais alvos de ataques por emails

Fonte: Abes (2022)

No que diz respeito aos ataques de ransomware, pode-se dizer que estes tiveram seu número dobrado em março de 2022, o que significou uma ascensão para quase 2,5 milhões em comparação a 1,2 milhão de ataques no mês de fevereiro do mesmo ano, o que tem gerado uma maior preocupação nos analistas de segurança. Segundo o autor, as grandes empresas continuam sendo o alvo preferido dos invasores, mas o Japão (20,6%) ficou em primeiro lugar à frente dos Estados Unidos (13,1%). Os cibercriminosos também têm como alvo o México (8,2%), Turquia (6,4%) e Índia (4,4%). Em 2021, um total de 14 milhões de ataques de ransomware foram identificados em todo o mundo (ABES, 2022).

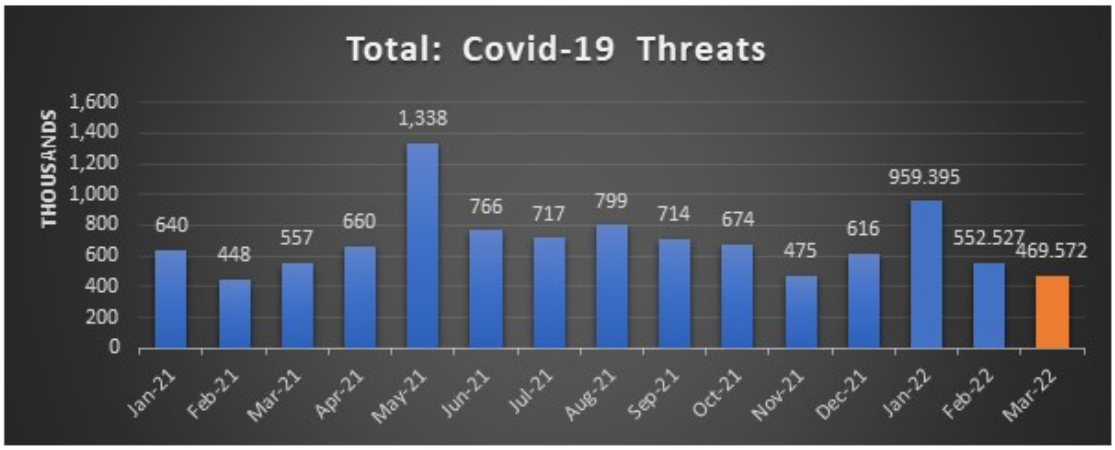
Imagem 3. Ataques de ransomware nos meses de fevereiro e março de 2022



Fonte: Abes (2022)

De acordo com a Abes (2022), a Trend Micro, até a data em que este trabalho foi escrito, continua monitorando ameaças relacionadas ao Covid-19, e ameaças que ocorrem desde o início da pandemia, utilizando palavras-chave. Após atingir o pico no segundo trimestre de 2021, janeiro deste ano teve um crescimento significativo com 959.000 registros. Porém, até o momento, pode-se observar que os ataques caíram significativamente, com 552 milhões de casos em fevereiro e cerca de 470 milhões em março.

Imagem 4. Total de casos relacionados e durante a pandemia da covid-19



Fonte: Abes (2022)

Pode-se observar através do mencionado anteriormente que a maioria das ameaças relacionadas ao Covid-19, aconteceram através de email (446 milhões), seguida por URLs maliciosos (quase 14 milhões). Ainda assim, a engenharia social com sites de email e phishing (9,8 milhões) é uma tática fundamental para os invasores. Infelizmente, o cenário para os países mais atingidos não mudou, com a maioria dos incidentes registrados no mês de março nos Estados Unidos e na Alemanha (ABES, 2022).

3.1. Protegendo-se da engenharia social

Mitnick e Simon (2003) afirmam que não existe tecnologia no mundo capaz de impedir um ataque de engenheiros sociais. No entanto, eles mencionam três elementos que trabalham juntos para diminuir as ameaças da engenharia social. Os autores citam que estes elementos são: a conscientização da segurança das informações pessoais e/ou de funcionários (no caso de uma empresa); educação e treinamento; e políticas de segurança, que estabelecem as principais regras que regem o comportamento dos usuários/funcionários.

Deve-se notar que as políticas de segurança devem ser muito específicas para proteger dados valiosos de indivíduos que, como remetentes, não são conhecidos pessoalmente e sim por serem "procedimentos de verificação de identidade" padronizados existenciais e dessa maneira, qualquer pessoa pode solicitar suas informações (COSTA et al., 2018).

Esses procedimentos devem ser uma extensão da política de segurança e devem incluir etapas claras para verificar a identidade de um solicitante, com diferentes níveis de autenticação dependendo do nível de sensibilidade das informações solicitadas (MITNICK e SIMON, 2003).

Ainda de acordo com os autores supracitados, as organizações não devem apenas estabelecer regras de política por escrito, mas também se esforçar para orientar todos que trabalham com informações corporativas ou sistemas de computador para aprender e seguir essas regras.

> Todos são tão vulneráveis aos ataques de Engenharia social que a única defesa efetiva de uma empresa é educar e treinar o seu pessoal, dandolhes a prática que precisam para identificar um Engenheiro Social. (MITNICK e SIMON, 2003).

De acordo com estes autores, um dos primeiros passos para um programa de conscientização eficiente é educar os funcionários por meio de sessões regulares de treinamento. Após completar o treinamento, é importante que sejam aplicadas técnicas

que sublinhem a importância de uma atitude responsável ao lidar com informações da empresa.

Um programa de conscientização deve ser constantemente atualizado. À medida que os engenheiros sociais descobrem novas técnicas, a área responsável por uma organização de educação em segurança deve estudar e atualizar seus funcionários sobre técnicas e métodos. Para isso, é fundamental realizar testes que avaliem se os programas estão produzindo os resultados esperados ou não (COSTA et al., 2018).

O primeiro passo do programa é conscientizar todos os funcionários de que existem indivíduos desonestos que os estão manipulando psicologicamente por meio de fraudes. Como explicam Mitnick e Simon (2003), uma vez que as pessoas tenham uma melhor compreensão de como podem ser manipuladas, é mais provável que reconheçam um ataque iminente. O programa deve se concentrar em conscientizar todos os funcionários de que sua organização pode ser atacada a qualquer momento e que a perda de informações confidenciais pode comprometer não apenas a empresa, mas também suas informações pessoais.

O programa de treinamento deve informar, engajar e inspirar os alunos e motivá-los a participar do programa e fazer sua parte para proteger os ativos de informação da organização. Ele visa transformar a conscientização e o treinamento de segurança da informação em uma experiência interessante e interativa (COSTA et al., 2018).

De acordo com a teoria do psicólogo americano Skinner, o comportamento ou motivação de uma pessoa é uma função das consequências desse comportamento quando somos recompensados com ele, por exemplo. determinado comportamento, iniciamos a conexão entre o comportamento adequado e o recompensador (COSTA et al., 2018).

A premissa básica dessa teoria é que o reforço condiciona o comportamento, que é determinado por experiências negativas ou positivas. O reforço positivo vem de várias formas, como: prêmios, promoções e até mesmo um simples elogio por um trabalho bem feito. Eles são motivadores porque incentivam a excelência. O reforço negativo força o funcionário a não se comportar de maneira desagradável, por meio de advertências até a demissão. (BOWDITCH e BUONO, 1992).

Com base nessa teoria, seria interessante premiar funcionários que consigam detectar e prevenir um ataque de engenharia social ou que promovam algum tipo de conscientização de segurança da informação na equipe. Em suma, qualquer ação tomada para garantir a segurança e eficácia do programa de conscientização deve ser reconhecida e recompensada. Da mesma forma, qualquer ação que facilite um ataque de engenharia social ou violação de regra deve ser devidamente repreendida para que seja desencorajada (GEWEHR, 2020).

De acordo com Saleem e Hammoudeh (2018), as políticas e procedimentos corporativos devem ser definidos e compartilhados para mitigar as ameaças de engenharia entre os funcionários de uma organização. Nesse sentido, é possível que mecanismos de segurança física e tecnológica falhem devido à proliferação de novas ações maliciosas. Portanto, em situações em que esses mecanismos falham, as políticas e procedimentos organizacionais podem ser a última linha de defesa da organização.

A Política de Segurança da Informação (PSI) é a ferramenta básica para formalizar procedimentos e políticas de segurança em uma organização. O PSI define diretrizes e limites para os controles a serem implementados, por isso este documento traz instruções e procedimentos que os colaboradores devem conhecer e aplicar, além de uma hierarquia que define quais informações cada usuário pode acessar e quais ações são tomadas em situações de necessidade emergencial. (FONTES, 2012).

Em suma, de acordo com a ABNT ISO/IEC 27002, o PSI deve incluir uma

definição de segurança da informação, seus objetivos globais, o escopo e a importância da segurança da informação e uma declaração de compromisso de gestão que apoie os objetivos e princípios de segurança. de informação. É responsabilidade das organizações garantir ampla divulgação e capacitação do PSI para os funcionários (FONTES, 2012).

No entanto, segundo Saleem e Hammoudeh (2018), quando os funcionários participam de um curso de treinamento, 50% esquecem o conteúdo após uma hora, 70% em 24 horas e 90% em uma semana. Nesse sentido, o treinamento em políticas e procedimentos de segurança deve fazer parte de um programa contínuo de conscientização e treinamento (ALDAWOOD; SKINNER, 2019).

De acordo Georgiadou, Mouzakitis e Askounis (2021), durante o período de pandemia causada pelo SARS-CoV-2, as empresas que apresentaram os melhores resultados de segurança implementaram a VPN (Virtual Private Network) como meio de comunicação. Adicionalmente, foram implementadas boas práticas de segurança, como por exemplo: proteger os emails com uma palavra-passe forte; a habilitação e a autenticação de dois fatores para email; a realização de backup de dados importantes com frequência e a proteção de smartphones e tablets com senhas de tela de bloqueio, além do uso do gerenciador de senhas (FURNELL; SHAH, 2020).

4. Considerações Finais

Foi observado que devido a todos os fatos e situações que aconteceram durante a pandemia, como por exemplo todas as medidas de higiene tomadas para conter o Covid-19 e milhares de pessoas trabalhando em casa, foi registrado um aumento importante no número de incidentes relacionados aos ataques de engenharia social, quando comparado ao ano de 2020.

Dessa maneira, pode-se dizer que o objetivo proposto do trabalho foi alcançado, a revisão de literatura realizada contribuiu para o entendimento dos diferentes tipos de ataques de engenharia social e a demonstração de práticas que podem ajudar o usuário a evitar ser atacado nesse formato.

Na sociedade moderna, as questões de segurança tornaram-se muito importantes. Apesar disso, muitas organizações esqueceram que seus próprios recursos humanos estão no centro da maioria das violações de segurança. As práticas de ataque incluem engenharia social, que requer muita pesquisa. A segurança do sistema não é apenas sobre a tecnologia em si, mas também sobre os processos por trás dela.

Diante disso, a tecnologia, por mais avançada que seja, não basta se os fatores humanos não forem considerados e preparados. As pessoas precisam estar cientes de que podem estar sendo observadas e se tornar um alvo potencial para engenheiros sociais que podem prejudicar a si mesmas e à empresa em que trabalham.

Referências

WERNER SILVA, L. Internet foi criada em 1969 com o nome de “Arpanet” nos EUA. Disponível em:https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml. Acesso em Outubro de 2021.

Wikipedia, História da Internet. Disponível em: https://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet. Acesso em Outubro de 2021.

Ministério das Comunicações e Ministério da Ciência e Tecnologia, Internet no Brasil. Disponível em: https://homepages.dcc.ufmg.br/~mlbc/cursos/internet/provedores_pol/intro.htm. Acesso em: Novembro de 2021

Tecmundo, A história das redes sociais. Disponível em: https://www.tecmundo.com.br/redes-sociais/33036-a-historia-das-redes-sociais-como-tudo-comecou.htm. Acesso em Outubro de 2021.

InfoEscola, Redes sociais. Disponível em: https://www.infoescola.com/sociedade/redes-sociais-2/. Acesso em Outubro de 2021.

Canaltech, A evolução das redes sociais e seu impacto na sociedade. Disponível em: https://canaltech.com.br/redes-sociais/a-evolucao-das-redes-sociais-e-seu-impacto-na-sociedade-parte-2-108116/. Acesso em Outubro de 2021.

ABES - Associação Brasileira das Empresas de Software. Trend Micro alerta: Brasil permanece na liderança do ranking de países que mais enviam ameaças de extorsão e sextorsão. 2022. Disponível em: <https://abes.com.br/trend-micro-alerta-brasil-permanece-na-lideranca-do-ranking-de-paises-que-mais-enviam-ameacas-de-extorsao-e-sextorsao/> Acesso em Setembro de 2022.

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. Acesso em Setembro de 2022.

DE LUCAS BASTOS, N. et al. Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus). Revista Tecnológica da Fatec Americana, v. 9, n. 01, p. 68-83, 2021.

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. Acesso em Setembro de 2022.

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. Acesso em Setembro de 2022.

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. Acesso em Setembro de 2022.

GEWEHR, R. Lembra-te de que vais morrer! Misérias da vida em comum em tempos de pandemia. Voluntas: Revista Internacional de Filosofia [Online], v. 11, p. 1-11, 2020.

JÚNIOR SILVA GUIMARÃES, D. et al. Efeitos da pandemia do COVID-19 na transformação digital de pequenos negócios. Revista de Engenharia e Pesquisa Aplicada, v. 5, n. 4, p. 1-10, 2020.

KASPERSKY (ed.). O que é phishing?. Brasil. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/vishing. Acesso em Setembro de 2022.

DUTRA NAGLI, L. S.. Pandemia na pandemia: a escalada de ataques cibernéticos pós COVID-19. In: Congresso Transformação Digital 2020. 2020.

PAZ, M; SANTOS, C. O FENÔMENO DOS GOLPES DIGITAIS DE ENGENHARIA SOCIAL E DO VAZAMENTO DE DADOS PESSOAIS NA PANDEMIA DA COVID-19. In: ABCIBER XIII-SIMPÓSIO NACIONAL DA ABCIBER 2020. 2021.

ROCHA, D. Engenharia social: compreendendo ataques e a importância da conscientização. 2020.Disponível em:<https://gatefy.com/pt-br/postagem/7-casos-reais-de-ataques-de-engenharia-social/>. Acesso em Setembro de 2022.

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

SANTOS, S. A Excecionalidade do Covid-19 e a Redefinição da Privacidade. IDN Brief, n. Especial Pandemia, p. 8-9, 2020.

MITNICK, Kevin D.; SIMON, William L. Mitnick. A Arte de Enganar - Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Makron Books, 2003, 286p.

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. Acesso em Setembro de 2022.

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. Acesso em Setembro de 2022.

MACKAY, J. Ataques De Engenharia Social a Ter Em Conta em 2022 e Mais Além. Janeiro de 2022.Disponível em: <https://www.metacompliance.com/pt/blog/phishing-and-ransomware/social-engineering-to-watch-out-for> Acesso em Setembro de 2022.

MACKAY, J. A Importância da Formação em Segurança Cibernética no Sector da Educação. Disponível em: <https://www.metacompliance.com/pt/blog/uncategorized/cyber-security-training-education-sector>. Acesso em Outubro de 2022.

MACKAY, J. Os Elementos de um Convincente Ataque de Phishing. Disponível em: <https://www.metacompliance.com/pt/blog/phishing-and-ransomware/elements-convincing-phishing-attack>. Acesso em Outubro de 2022.

MACKAY, J. Os Perigos do Resgate de Ransomware. Disponível em: <https://www.metacompliance.com/pt/blog/cyber-security-awareness/the-dangers-of-ransomware>. Acesso em Outubro de 2022.

Leadcomm. Como os cibercriminosos estão atacando durante a Pandemia de COVID-

19? Disponível em: <https://leadcomm.com.br/2020/07/21/como-os-cibercriminosos-estao-atacando-durante-a-pandemia-do-covid-19/>. Acesso em Outubro de 2022.