FATEC SÃO CAETANO DO SUL – ANTONIO RUSSO
SEGURANÇA DA INFORMAÇÃO

FABRICIO BIAZZOTTO
FREDERICO AZEVEDO ANTICOLI
GUSTAVO VILELA BOCCIA

UTILIZAÇÃO DA TECNOLOGIA PARA MITIGAR OS ATAQUES DE ENGENHARIA SOCIAL EM AMBIENTES CORPORATIVOS

SÃO CAETANO DO SUL – SP
2020

FABRICIO BIAZZOTTO
FREDERICO AZEVEDO ANTICOLI
GUSTAVO VILELA BOCCIA

UTILIZAÇÃO DA TECNOLOGIA PARA MITIGAR OS ATAQUES DE ENGENHARIA SOCIAL EM AMBIENTES CORPORATIVOS

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de São Caetano do Sul, sob a orientação do Professor Me. Kleber Divino da Silva, como requisito parcial para a obtenção do diploma de Graduação no Curso de Tecnologia em Segurança da Informação.

SÃO CAETANO DO SUL – SP
2020

RESUMO

ANTICOLI, Frederico A. BIAZZOTTO, Fabricio. BOCCIA, Gustavo V. **Utilização da tecnologia para mitigar os ataques de engenharia social em ambientes corporativos**. 13 f. Trabalho de Graduação – Faculdade de Tecnologia de São Caetano do Sul, São Caetano do Sul, 2020.

O presente trabalho tem como meta expor os pilares da engenharia social com o propósito de evidenciar como a tecnologia potencializou os riscos neste âmbito. Abordar a Ameaça Persistente Avançada (APT) e sua principal forma de ataque, direcionado às grandes corporações, conhecido como Comprometimento de E-mail Corporativo (BEC). Apresentar três *softwares* de mercado que procuram reduzir as vulnerabilidades relacionadas com este ataque específico afim de impedir que os engenheiros sociais tenham êxito contra seus alvos. Finalmente, comparar suas características e diferenciais com o escopo de responder se tais ferramentas são capazes de mitigar o risco integralmente.

Palavras-chave: engenharia social; ameaça persistente avançada; comprometimento de e-mail comercial.

ABSTRACT

ANTICOLI, Frederico A. BIAZZOTTO, Fabricio. BOCCIA, Gustavo V. **Use of technology to mitigate social engineering attacks related to corporate environments.** 13 f. Trabalho de Graduação – Faculdade de Tecnologia de São Caetano do Sul, São Caetano do Sul, 2020.

The present work aims to expose the pillars of social engineering in order to show how technology has enhanced the risks in this area. Addressing Advanced Persistent Threat (APT) and its main form of attack, directed at large corporations, known as Business E-mail Compromise (BEC). Present three software that seek to reduce the vulnerabilities related to this specific attack for prevent social engineers from succeeding against their targets. Finally, compare their characteristics and differentials with the scope of answering whether such tools are capable of completely mitigate the risk.

Keywords: social engineering; advanced persistent threat; business email compromisse.

SUMÁRIO

INTRODUÇÃO

A tecnologia pode ser alterada, porém o fator mais influente em segurança – o usuário final – não. “Porque, no fim, o elo mais fraco em todas as coisas é a pessoa(...)”, conforme elucida Schwartau (2010), consultor de segurança da informação por mais de 25 anos, fundador da Security Awarness Company.

Portanto, antes mesmo de falar de computação ou até mesmo de Segurança da Informação (SI), é primordial construir uma visão holística sobre como o ser humano está exposto do ponto de vista da engenharia social e consequentemente, como as vulnerabilidades e potenciais riscos associados têm sido explorados na atualidade.

A Trend Micro (2019), gigante no setor de proteção contra ameaças cibernéticas, esclarece em seu *website* uma delas ao falar sobre o ataque do tipo *Business E-Mail Compromise* (BEC), Comprometimento de E-mail Corporativo, em tradução livre. É um tipo de golpe destinado a empresas e executivos que realizam transferências bancárias e têm fornecedores espalhados no exterior. Contas de e-mail corporativas de executivos ou funcionários de alto nível relacionadas a finanças ou envolvidas com pagamentos por transferência eletrônica ou publicamente disponíveis são falsificadas ou comprometidas por *keyloggers*, *scanner* de digitação, ou ataques de *phishing*, e-mails falsos que visam infectar o destinatário, para realizar transferências fraudulentas, resultando em perdas de centenas de milhares de dólares.

Daí surgiu o tema norteador e premissa de estudo neste trabalho, o uso de tecnologias para minimizar ataques de engenharia social em ambientes corporativos.

Indivíduos possuem sensações que estão associadas a percepções e que geram emoções, e cada uma, certa visão de mundo (MYERS, 1999). Consequentemente outros podem enxergar tais comportamentos como brechas, fraquezas, de modo a tirar vantagem para se beneficiarem. Nesse sentido, a engenharia social tem como base principal a confiança de quem a aplica, por meio dela podemos assumir identidades de terceiros e fazer o que vier à mente. São inúmeros casos em que pessoas obtiveram acesso a informações sigilosas simplesmente por passarem firmeza e clareza em suas mentiras.

Quando se dá crédito a alguém, automaticamente temos a sensação de ter um elo com essa criatura, e é natural na maioria das vezes querer ser útil ou gentil ajudando o outro, acontece que nem todas as pessoas possuem boas intenções, e é onde o perigo se esconde.

Em 1928, o Dr. William Moulton Marston escreveu um livro chamado "*Emotions of Normal People*", que chegou a ser traduzido somente em 2014 com o título de “As emoções das pessoas normais”, onde ele determina alguns padrões de comportamento.

Em sua obra, é desenvolvida a metodologia DISC:

D – Dominância (forma de lidar com desafios e problemas);

I – Influência (forma de lidar com influência de terceiros);

S – Estabilidade (forma de lidar com mudanças);

C – Conformidade (forma de lidar com a aceitação de procedimentos e regras estabelecidos por outros).

A ideia principal é que cada ser humano possui uma individualidade, uma singularidade, mas podemos ser facilmente compreendidos por um ou dois estilos de comportamento descritos acima, os quais se destacam frente ao conjunto. Assim, combinando com o ímpeto dos outros estilos, é definido nosso estilo real de comportamento geral.

Em 1999, David G. Myers escreveu um livro chamado Introdução à Psicologia Geral onde aborda uma introdução para psicologia e seus conceitos. Em um primeiro momento, este tema parece bem distante da engenharia social, porém é notável que ambos se baseiam nos mesmos conceitos. Todos temos necessidades humanas básicas, elas são:

- Desejo por reciprocidade – se eu faço por ti, automaticamente você tem que ser gentil e fazer por mim;
- Desejo de aprovação social – Se a maioria acredita, então é a opção certa;
- Pré-julgamento de autoridades – Policiais, médicos, técnicos (ambos com fardas e uniformes de trabalho).

Um caso famoso envolvendo engenharia social ocorreu em 2003 (Jornal Extra Online, 2016) no Brasil, foi executado por Carlos da Cruz Sampaio Júnior, um homem que se passou por tenente-coronel de polícia no estado do Rio de Janeiro.

Carlos foi segurança de um zoológico e já possuía bastante conhecimento sobre os processos da academia, pois seu pai era capitão do exército brasileiro. Através da confiança que ele desenvolveu ao longo de sua vida, se apresentava com tal patente, chegando inclusive a fazer parte de operações especiais e sigilosas, dar palestras e até mesmo treinos bélicos para militares, durante quatro anos, em momento algum foi questionado sobre sua identidade. Em outubro de 2010, após apresentar documentos falsos, acabou sendo condenado por porte ilegal de arma e indiciado por outros crimes relacionados com sua farsa.

OBJETIVO

Este trabalho tem por objetivo apresentar e comparar três *softwares* de mercado que procuram impedir o ataque de engenharia social às corporações conhecido como Comprometimento de E-mail Corporativo (BEC), uma das principais formas de ataque do tipo Ameaça Persistente Avançada (APT).

OBJETIVO ESPECÍFICO

Para alcançar o objetivo central deste trabalho, os seguintes objetivos específicos serão traçados:

- Aprofundar os conceitos da psicologia afim de compreender como a mente humana absorve certas emoções e constrói sentimentos fazendo um paralelo com as vulnerabilidades que a engenharia social explora.
- Levantar quais são as ameaças conhecidas e como evoluíram após a era da informação, principalmente nos recentes ataques direcionados aos executivos de grandes empresas.
- Avaliar as três ferramentas, suas características, aspectos de implementação e os diferenciais com a finalidade de responder se são suficientes para proteger os ativos que são alvo destes ataques.
- Responder se estes softwares são suficientes para mitigar o ataque de APT conhecido por BEC.

JUSTIFICATIVA

O APT é uma ameaça que vem sendo cada vez mais utilizada em ataques via e-mail, sendo inclusive citada por Kasey Panetta na *Gartner Top 10 Security Projects for 2019*, uma das maiores empresas de referência em SI, a partir dele surgiu a ideia de estudarmos o tema de *Comprometimento de E-mail Corporativo* (BEC).

Um projeto de comprometimento de *e-mail* comercial pode ajudar os líderes de segurança e risco a lidarem com ataques de *phishing* e processos de negócios mal definidos. Esses projetos se concentram em controles técnicos, bem como em falhas de processos críticos da organização. Opções personalizáveis de aprendizado de máquina podem ser integradas aos sistemas de segurança de *e-mail* e os líderes de segurança e risco podem também procurar os provedores de segurança de *e-mail* atuais para fornecer esses controles, além de integrar o projeto ao treinamento de conscientização de segurança e outras proteções de terminais.

RELEVÂNCIA

A partir dos estudos, será possível responder se as ferramentas existentes no mercado são suficientes para garantir a segurança dos e-mails corporativos. Consequentemente, visualizar se as corporações estão protegidas ao utilizarem estes softwares ou serão necessárias novas abordagens e/ou desenvolvimentos complementares para mitigar os riscos e impactos em caso de ataques reais.

PROBLEMATIZAÇÃO

A era da informação trouxe inúmeros benefícios, mas juntamente com o progresso da tecnologia, proporcionalmente as ameaças se tornaram mais sofisticadas. Especialmente, os ataques de engenharia social via e-mail e direcionados principalmente para grandes corporações. Assim, buscaremos responder se as ferramentas atuais no mercado são suficientes para mitigar este tipo de risco.

HIPÓTESES

As ferramentas existentes não são suficientes, na realidade são apenas uma parcela dos controles necessários para redução integral do risco associado aos ataques, pois há diversas vertentes possíveis, como *e-mail*, ligação, corpo-a-corpo, entre outros. É necessário conscientização e abordagens específicas para cada tipo de indivíduo e corporação.

METODOLOGIA

A engenharia social é um dos meios mais prolíficos e eficazes para obter acesso aos sistemas seguros e obter informações confidenciais, ainda requer conhecimento técnico mínimo. Os ataques variam de e-mails do tipo *phishing* com pouca sofisticação, até ataques altamente direcionados e de inúmeras camadas, que usam uma ou diversas técnicas combinadas. Tal técnica funciona manipulando humanos diretamente no que tange o comportamento e, como tal, existem apenas soluções técnicas limitadas para se proteger.

A melhor defesa é educar o usuário sobre a maneira que os engenheiros sociais trabalham e aumentar assim a conscientização sobre como os indivíduos e os sistemas de computador podem ser manipulados para criar um falso nível de confiança. Esta pode ser complementada por uma atitude organizacional em relação a defesa e que promova o compartilhamento de casos situacionais passados ou simulados educacionais, com os controles e técnicas de segurança da informação e lições aprendida, assim incentivar os usuários e sua utilização e suporte em relação à aderência.

Com isso, será realizada uma pesquisa bibliográfica com base nas ameaças do tipo APT e os ataques do tipo BEC, que compreenda os conceitos necessários para o desenvolvimento do trabalho.

Após a busca, serão analisadas e comparadas três ferramentas disponíveis, analisando seus aspectos, características e diferenciais. Com os resultados obtidos espera-se trazer uma contribuição para área corporativa pela disponibilização de informações consolidadas sobre meios de identificação, redução e prevenção dos ataques de engenharia social.

Este trabalho de conclusão de curso é composto de 4 capítulos: o capítulo 1 - Engenharia Social Antes da Era da Informação, trata da engenharia social, os pilares da oratória e sua relação com a psicologia; O capítulo 2 – A Era da Informação, apresenta como as técnicas de engenharia social utilizadas até então se transformaram com o avanço da tecnologia; O capítulo 3 - Ameaças, aborda como as ameaças estão relacionadas com as vulnerabilidades que a era da informação proporcionou; O capítulo 4 – *Advanced Persistent Threat*, estuda as ferramentas que buscam mitigar a ameaça do tipo APT e o ataque do tipo BEC; Finalmente trazendo nas considerações finais qual foi a conclusão obtida após esta jornada.

1. ENGENHARIA SOCIAL ANTES DA ERA DA INFORMAÇÃO

Basicamente, engenharia social refere-se à manipulação psicológica dos seres humanos e no contexto de SI, é a arte de explorar usuários para comprometer os sistemas de informação. O foco desses ataques são primeiramente pessoas ao invés de ataques técnicos aos sistemas de informação.

Os engenheiros sociais tentam manipular suas vítimas para divulgar informações confidenciais ou realizar seus objetivos maliciosos usando influência e persuasão. Assim, as formas de ataques muitas vezes tornam ineficazes as medidas de proteção técnica. As pessoas, em geral, pensam que são boas na detecção desses ataques. Pesquisas, no entanto, indicam que as pessoas têm um desempenho ruim na detecção de mentiras e decepções (MARETT, 2004).

Na área de tecnologia e informática, a engenharia social é discutida principalmente com exemplos de casos reais que comprovam quão devastadores ataques sofisticados podem ser para a segurança da informação de empresas e organizações governamentais. No entanto, o campo de psicologia social aborda importantes descobertas sobre os princípios de persuasão. Especialmente o trabalho de CIALDINI (2001), especialista no campo da persuasão, frequentemente citado em contribuições para pesquisa em engenharia social. Embora Cialdini traga um modelo de persuasão com base no marketing, seus princípios são cruciais para entender como a arte da enganação funciona.

Não é preciso refletir muito para constatar que manipular pessoas não depende do computador, diversas técnicas já existem há muitos anos e foram aprimoradas ao longo do tempo. Se é certo que a comunicação pode ser exercida de múltiplas formas e obedecendo diversas intencionalidades, não é menos verdade que o acontecimento comunicacional se inscreve sempre num ato relacional. Com efeito, esta antiga disciplina sempre existiu para se debruçar sobre as relações comunicativas. Originalmente, para atentar sobre o relacionamento, então necessária e exclusivamente discursivo, entre as pessoas.

1.1 OS TRÊS PRINCIPAIS PILARES DA ORATÓRIA

Na Grécia antiga, Aristóteles, que viveu em 384 a 322 a.C, formalizou uma obra chamada "Retórica", que é dividida em três partes: Elaboração da mensagem (Logos, prova lógica - Livro 1), provas ou meios de persuasão (Pathos, emoção e caráter - Livro 2) e Estilo e composição do discurso (Ethos, Livro 3).

Segundo o livro Retórica, Aristóteles afirmou que a retórica era compreendida como a capacidade de descobrir o que é adequado a cada caso com o fim de persuadir. Para ele, essa vertente do saber se manifesta como uma metodologia única, pela situação de ter a faculdade de descobrir os meios de persuasão sobre qualquer questão dada (PENA, 2015).

De acordo com a tradição da Grécia, a retórica é dissecada em quatro partes que, como afirma Reboul (2004) "representam as quatro fases pelas quais passa quem compõe um argumento, ou pelas quais, acredita-se que passe". Assim, um processo argumentativo por inteiro, deveria ser desenvolvido em quatro etapas:

- Invenção;
- Disposição;
- Elocução;
- Ação.

Essas etapas acima consistem em: compreender o assunto apresentado e juntar todos os argumentos pertinentes (invenção); pô-los em ordem (disposição); elaborar o discurso da melhor forma possível (elocução); articular (ação).

Esses quatro ciclos podem ser compreendidos como quatro "afazeres" a serem seguidos, se assim o fizer, sua fala e/ou discurso será infalível, assim com menos suscetível de tornar-se vazio, sem sentido ou até mal elaborado (REBOUL, 2004).

De acordo com o povo grego, o ente[1] que tiver o propósito de elaborar um discurso eficaz, deve passar por essas quatro fases, ou pelo menos, buscar exercer o que cada uma delas representa. Como nos lembra Ferreira (2010), o discurso em

[1] "O que existe ou é forma concreta ou objetiva. Coisa, Entidade, Ser, Substância." https://dicionario.priberam.org/ente.

nossos dias, não se constrói por formas rígidas ou mecânicas, como divulgavam os antigos.

Conforme Aristóteles (1979, p. 23), o *Logos* diz respeito ao uso da lógica, ou seja, a forma como o assunto é apresentado (clareza no discurso, ordem dos argumentos ou até mesmo o uso de falácias).

De acordo com livro Retórica (2015, p. 24), os apelos lógicos baseiam-se em modos racionais de pensamento, são eles:

- Comparação entre duas coisas semelhantes, para ajudar a apoiar sua reivindicação. É importante que a comparação seja justa e válida. As coisas que estão sendo comparadas devem compartilhar traços significativos de similaridade.
- Pensamento de causa / efeito - você argumenta que X causou Y ou que X provavelmente causará Y para ajudar a apoiar sua reivindicação.
- Raciocínio dedutivo - começando com uma reivindicação/exemplo geral amplo e usando-a para apoiar um ponto ou reivindicação mais específica.
- Raciocínio indutivo - usando vários exemplos ou casos específicos para fazer uma ampla generalização.
- Exemplificação - uso de muitos exemplos ou várias evidências para apoiar um único ponto.
- Elaboração - indo além da inclusão de um fato, mas explicando a importância ou a relevância desse fato.
- Pensamento coerente - mantendo uma linha de raciocínio bem organizada; não repetindo ideias ou pulando.

Conforme Aristóteles (1979, p. 25) o *Ethos* aborda os atributos da ética, ela é a percepção que o público tem sobre sua boa moral e sua autoridade. O caráter é outro aspecto do *ethos*, que difere da credibilidade porque envolve história pessoal e até traços de personalidade. Uma pessoa pode ser credível, mas não possui caráter ou vice-versa, assim, o *ethos* se resume à confiança. Ao criar apelos éticos, vemos os seguintes pontos:

- Referir-se direta ou indiretamente aos valores que importam para o público-alvo (para que o público confie nele)

- Usando linguagem, fraseado, imagens ou outros estilos de escrita comuns às pessoas que detêm esses valores, “conversando sobre o assunto” das pessoas com esses valores (novamente, para que o público ou alvo crie confiança)
- Referindo-se à sua experiência e/ou autoridade com o tópico (assim, portanto, demonstrando sua credibilidade)
- Referindo-se ao próprio personagem ou fazendo um esforço para criar seu personagem no contexto.

Por fim, o *Pathos* refere-se ao lado emocional (CARVALHO, 1979).

Ainda conforme Carvalho (1979) quando uma pessoa confia em seu *Pathos*, significa ela está tentando aproveitar as emoções do público para fazê-la concordar com a sua afirmação. Estratégias retóricas baseadas no *pathos* são aquelas que levam o público a "se abrir". As emoções podem nos tornar vulneráveis, e um engenheiro pode usar essa vulnerabilidade para fazer com que o público acredite que seu argumento é convincente.

Por exemplo, podemos citar ataques que através de telefonemas[2], que buscam brechas emocionais simulando entes queridos em cenários infelizes.

Segundo Carvalho (2020), estes campos da emoção podem incluir:

- Descrições expressivas de pessoas, lugares ou eventos que ajudam o alvo a sentir à vontade.
- Imagens vívidas de pessoas, lugares ou eventos que ajudam a vítima sentir-se que está neste lugar novamente.
- Compartilhar histórias pessoais que fazem o alvo sentir uma conexão ou empatia.
- Usar o vocabulário carregado de emoções como uma maneira de colocar a pessoa nessa mentalidade emocional específica.
- Usando qualquer informação que evoque uma resposta emocional. Isso pode envolver fazer com que a vítima sinta empatia ou repulsa pela

[2] "Presidiários aplicam golpes por telefone; Saiba como se proteger. http://g1.globo.com/jornal-nacional/noticia/2017/07/presidiarios-aplicam-golpes-por-telefone-saiba-como-se-proteger.html.

pessoa/grupo/evento que está sendo discutido, ou talvez conexão ou rejeição.

Entendendo estes três pilares e explorando-os da maneira adequada, podemos manipular as pessoas conforme nosso querer.

Segundo Hadnagy (2011), a engenharia social é “uma arte, ou melhor que isso, a ciência, de manipular os seres humanos para agir em algum aspecto de suas vidas." Quanto mais tempo o engenheiro social estuda sobre o alvo, maior pode ser seu sucesso, ou seja, quanto mais informações sobre o alvo, mais fácil será, sem mencionar o fato que ao possuir este leque de informações, mais opções estarão abertas.

Kevin Mitnik (2002, p. 16) define:

> "(...) A quantidade de informações é um ponto chave para que todo o processo obtenha êxito, pois quanto mais familiar se parece o engenheiro, mais à vontade o alvo se sente para entregar informações relevantes. A partir do pretexto criado, é estabelecido certa confiança entre as duas partes, abrindo espaço para a influência. A taxa de triunfo depende desses dois fatores."

Através da psicologia, Cialdini (2017) define algumas técnicas:

- Reciprocidade - o instinto de que "uma boa parte merece outra";
- Obrigação - A compulsão natural de responder a certas ações e normas sociais - por exemplo, responder a uma pergunta principal com a resposta esperada;
- Concessão - Ao conceder uma questão menor, um engenheiro social pode obter simpatia e aumentar a probabilidade de concessões recíprocas do alvo;
- Escassez - Muitos ataques de engenharia social invocam a escassez de um recurso, como tempo ou dinheiro, para influenciar seus alvos;
- Autoridade - Estudos como o "experimento de Milgram" mostraram a disposição das pessoas de se submeterem a figuras de autoridade, mesmo quando sabem que a ação que são solicitadas a executar é contrária às suas crenças.

Conforme Hadnagy (2011) elucida, se um engenheiro social é capaz de criar um relacionamento com seu alvo, é muito mais provável que ele atinja seu objetivo. Os engenheiros sociais usam muitas técnicas também usadas por vendedores e executivos de sucesso para isso. Incluindo escuta ativa, técnicas eficazes de questionamento e licitação e um bom conhecimento dos interesses de seus alvos. Técnicas mais sutis podem incluir combinar o visual ou a aparência do alvo ou espelhar seus padrões de fala e linguagem corporal.”

1.2 CONSENSO OU PROVA SOCIAL

Conforme Cialdini (2011), eles demonstraram o 'efeito halo', em que a atratividade social de um indivíduo resulta em um viés a seu favor em outras áreas dos sentimentos do observador. Isso geralmente é demonstrado pela tendência das pessoas a aprovar mais pessoas que acham atraentes ou que se parecem com elas, independentemente de seu desempenho empírico. Os efeitos do halo ocorrem porque a percepção social humana é um processo altamente construtivo. Como os humanos formam impressões das pessoas, eles não confiam simplesmente em informações objetivas, mas constroem ativamente uma imagem coerente e significativa que se encaixa no que já sabem. Essa tendência a formar impressões significativas, bem formadas e consistentes também é confirmada por outros estudos concebidos dentro da tradição teórica da Gestalt. Apresentando-se visual e confortavelmente como atraente para seus objetivos, os engenheiros sociais podem ganhar credibilidade e aumentar suas chances de sucesso.

Após apresentar os conceitos da psicologia e sua relação direta com a engenharia social, seus pilares e características, será abordado no próximo capítulo como a era da informação aumentou a superfície de ataque e potencializou as vulnerabilidades e riscos para pessoas e organizações.

2. A ERA DA INFORMAÇÃO

Com relação aos esforços para mitigar os ataques dos engenheiros sociais, Mitnick afirmou: “A verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social” (MITNICK; 2003, p. 195).

O Primeiro vírus de computador não foi uma grande ameaça. Criado por Elk Cloner, que era um estudante do ensino médio de Pittsburgh, ele conseguiu irritar os usuários do Apple II com um simples poema.

Com o passar do tempo, esses ataques foram mudando, não era simplesmente algumas brincadeiras de mal gosto (como o ILOVEYOU[3], que ao abrir um arquivo de texto deletava suas imagens), eles passaram a roubar dados e ocasionalmente pedir uma certa quantia para o resgate dos mesmos. A seguir explicamos alguns ataques relacionados a engenharia social com o computador que abrangem todas as faces de um ataque onde o fator humano está envolvido, seja em qualquer etapa.

2.1 TIPOS DE ENGENHARIA SOCIAL

Os ataques de engenharia social são multifacetados e incluem: aspectos físicos, sociais e técnicos usados em diferentes estágios do ataque real. Esta subseção visa explicar as diferentes abordagens usadas pelos atacantes (ALVES, 2020).

2.1.1 ABORDAGENS FÍSICAS

Conforme explica Cassio Alves Bastos (2020), com ataques físicos, como o nome indica, o atacante realiza alguma forma de ação física para reunir informações sobre uma futura vítima, que podem variar de informações pessoais (número do CPF, data de nascimento) para credenciais válidas para um sistema de computador.

Uma técnica comum é pesquisar o lixo de uma organização, também conhecido como mergulho no lixo (seja físico ou virtual). Este lixo, pode fornecer

[3] "ILOVEYOU – foi um vírus de computador que afetou mais de 50 milhões de computadores Windows em 5 de maio de 2000.

informações valiosas para invasores, como dados pessoais sobre funcionários, manuais, memorandos e até impressões de informações confidenciais, como as credenciais do usuário (GRANGER, 2001).

Um invasor também pode tentar visualizar se no ambiente do escritório há informações relevantes como senhas escritas em *post-its* ou documentos sobre as estações de trabalho. Ataques menos sofisticados desse tipo envolve roubo ou extorsão para obter informações (CIAVATTA, 2019).

2.1.2 ABORDAGENS SOCIAIS

Obviamente, ataques sociais são a faceta mais emergente de engenharia social que utiliza técnicas sociopsicológicas como os princípios de persuasão de Cialdini (2011). De acordo com Granger (2001) o tipo mais prevalente desses ataques sociais é realizado por telefone. Para aumentar as chances desses ataques, os autores tentam desenvolver um relacionamento com suas futuras vítimas.

2.1.3 ENGENHARIA SOCIAL REVERSA

Em vez de entrar em contato com a vítima, os atacantes podem tentar fazer com que as vítimas peçam ajuda delas (GRANGER, 2001).

Conforme Nelson (2008), essa abordagem indireta é conhecida como “engenharia social reversa” e consiste em três partes principais: sabotagem (criar o problema); publicidade (anunciar que consegue resolvê-lo) e assistência (auxiliar na resolução do problema que foi criado anteriormente).

2.1.4 ABORDAGENS TÉCNICAS

As faces técnicas dos ataques são realizadas principalmente na Internet. Sarah Granger (2001) cita que a Internet é especialmente interessante para os engenheiros sociais coletarem senhas, devido ao fato de que os usuários frequentemente repetem as mesmas senhas para contas diferentes.

Além disso, a maioria das pessoas não está ciente que fornecem muitas informações pessoais de graça, o que é útil para os atacantes, e em posses destes dados, futuras vítimas podem ser selecionadas (VANHEUANGDY, 2010), sem contar as redes sociais que também contém inúmeras informações úteis.

2.1.5 ABORDAGENS SOCIOTÉCNICAS

Ataques bem-sucedidos de engenharia social costumam usar as diferentes faces discutidas até agora em combinação. No entanto, abordagens sociotécnicas permitiram a transformação das armas mais poderosas dos engenheiros sociais. Os exemplos incluem o chamado *baiting*, invasores deixam a mídia de armazenamento infectada por *malware* em um local onde é provável que seja encontrado por futuras vítimas.

Poderiam, por exemplo, ser *pendrives* contendo um Cavalo de Tróia (STASIUKOSIS, 2006). Além disso, os atacantes estão explorando a curiosidade das pessoas adicionando rótulos tentadores a essas mídias de armazenamento. Tal como “Confidencial” ou “Fotos íntimas”. Outra combinação comum de abordagens técnicas e sociais é o *phishing*. O *phishing* normalmente envolve e-mail ou mensagens instantâneas e em comparação com a engenharia social, é semelhante ao *spam* que é disparado para um grande grupo de usuários. A engenharia social, por outro lado, normalmente é direcionada a pessoas solteiras ou pequenos grupos de pessoas. Os golpistas esperam que, pelo vasto número de mensagens que eles enviam aos usuários, pessoas suficientes se enganem e tornem seu ataque de *phishing* lucrativo. Herley e Florencio (2008) argumentam que o *phishing* clássico não é lucrativo, o que pode explicar por que os ataques de *phishing* estão se movendo para ataques de *phishing* mais sofisticados. Os ataques *SpearPhishing* são mensagens altamente direcionadas após a mineração de dados inicial em redes sociais usadas, sites para extrair dados de alunos que, em seguida, receberam uma mensagem que parecia ser enviada por um amigo da vítima.

Os autores mostraram que eles poderiam aumentar o *phishing* com taxa de sucesso anterior de 16% para 72% usando esses "dados sociais". Portanto, o *SpearPhishing* pode ser visto como um casamento de engenharia social e tecnologia.

2.2 PRECAUÇÕES

Algumas recomendações para diminuir as vulnerabilidades e como consequência, reduzir riscos:

1. **Use senhas fortes**: Usar senhas fortes é uma das maneiras básicas de prevenção de ataques de engenharia social. Uma senha forte deve conter uma combinação de letras maiúsculas e minúsculas, números, símbolos e preferencialmente no mínimo 8 caracteres.

2. **Use senhas diferentes:** De acordo com uma pesquisa realizada por Truta (2018), aproximadamente 59% das pessoas usam as mesmas senhas para diferentes contas, o que facilita a invasão de suas contas por *hackers* mal-intencionados. Quando descobrem uma, descobrem todas.

3. **Use autenticação de dois fatores:** Muitos sites de mídia social como Facebook, Instagram, WhatsApp permitem o uso da Autenticação de Multi Fator (MFA) para proteger seus usuários de serem *hackeados* (ALVES, 2010).

4. **Evite visitar sites suspeitos:** Nunca visite um site suspeito, sem certificado digital ou clique em *links* desconhecidos. Isso pode direcioná-lo para páginas infectadas (ALVES, 2010).

5. **Nunca abra um e-mail de uma pessoa desconhecida:** A maioria dos ataques de *phishing* e isca são feitos apenas através de e-mails e basta abri-los para ser infectado (PEIXOTO, 2006).

6. **Instale o Antivírus:** instalar um antivírus e mantê-lo atualizado pode proteger seu computador de qualquer tipo de *malware* que o invasor tente instalar em seu computador através de engenharia social (ALVES, 2010).

7. **Verifique sempre a URL antes de visitar qualquer site:** Deve-se sempre verificar a URL, pode ser traduzida para o português como Localizador Uniforme de Recurso, antes de usar o site. Os sites que têm certificado SSL (HTTPS) instalado neles são considerados seguros (ALVES, 2010).

8. **Nunca dê seu telefone ou computador a qualquer pessoa não confiável:** De acordo com Mitnik (2018), impedir que qualquer terceiro use seu telefone ou computador é um dos melhores métodos de prevenção de engenharia social.

9. **Nunca insira nenhuma unidade *flash* desconhecida:** Muitas pessoas anexam dispositivos USB de lugares desconhecidos que contêm *malware*, com isso ajudam um invasor a assumir o controle total de seu sistema, nunca insira uma unidade desconhecida em seu computador pessoal (STASIUKOSIS, 2006).

10. **Alterar senhas com frequência:** Conforme recomenda Truta (2018), é preciso alterar a senha de sua conta seja contas de mídia social ou contas bancárias, as senhas devem ser alteradas com frequência, preferencialmente a cada trimestre.

11. **Conscientização crescente sobre Engenharia Social:** Um dos melhores métodos para prevenir a engenharia social é educar as pessoas sobre o tema e como ela é potencialmente danosa (MITNICK, 2002).

É importantíssimo compreender como a era da informação transformou as práticas de influência e persuasão, e ainda compreender que tais precauções são um esforço para reduzir a superfície de ataque com objetivo de aproximar de zero as chances de uma vulnerabilidade ser explorada (CIALDINI, 2001). Assim podemos partir para o estudo das ameaças no capítulo seguinte.

3. AMEAÇAS

Segundo o Instituto SANS, em seu glossário, temos a seguinte definição (em tradução livre) para ameaça[4]: "Uma potencial violação da segurança, que existe quando há circunstância, capacidade, ação ou evento que poderia quebrar a segurança e causar danos."

Na visão de Peixoto (2006), as ameaças são consequências naturais das vulnerabilidades existentes, o que mostra que um ou mais elementos fundamentais para existir segurança da informação: confidencialidade, integridade e disponibilidade, são passíveis de serem comprometidos. Essas ameaças podem ser divididas em:

- Naturais: Fenômenos da natureza como por exemplo as descargas elétricas ou enchentes etc.

- Involuntárias: Ocorrem por erro não proposital, desconhecimento ou acidentes.

- Voluntárias: São aquelas onde há intenção real de explorar uma brecha, propositais e resultado de ações dos engenheiros sociais por exemplo.

O foco das ameaças a seguir, será direcionado para as que são provenientes da ação intencional de uma pessoa ou grupo. Na última década, vimos um grande aumento no uso da Internet em todo o mundo e agora quase todas as empresas têm presença online. O aumento dramático de usuários domésticos e empresariais tornou o mundo digital mais complexo e, como resultado, os riscos à segurança se tornaram mais comuns e sofisticados. Com este abrupto crescimento, as mídias sociais cresceram exponencialmente e conquistaram seu espaço, consequentemente, os ataques dentro destas plataformas também.

[4]"Glossary of Security Terms - SANS Institute." https://www.sans.org/security-resources/glossary-of-terms/. Data de acesso: 21 jun.. 2020.

3.1 MÍDIA SOCIAL

Uma pesquisa revela que 25% dos usuários do Facebook não se preocupam com as configurações de privacidade (BULLAS, 2014).

Conforme de Bullas (2014) "A mídia social é considerada a principal ameaça devido sua popularidade e crescente diversidade."

As redes sociais conectam pessoas, mas através das cadeias de amigos e conhecidos, acompanhadas por um perfil convincente, diferentes solicitações de amizade podem se tornar o melhor caminho para um terreno fértil no vazamento de informações e, com a ajuda de um sistema de baixa segurança, podem até derrubar grandes empresas (GUNATILAKA, 2011).

3.2 MALWARE

O *malware* provém de *malicious software* (software malicioso, em tradução livre). Uma pesquisa mostra que 36% das empresas tiveram seus sistemas infectados com *malware* através da mídia social 2009, enquanto aumentou para 70% em 2010 (VANHEUANGDY et al, 2010).

Muitos são os *links* que circulam dentro destas páginas de internet. Por exemplo, em alguns deles pode ser necessário fazer um *download* ou atualizar o *Flash Player*, ao aceitar baixar ou apenas atualizar este *software* no computador do usuário, será infectado com *worms* que podem danificar o sistema (GUNATILAKA, 2011). Descoberto em 2008, um vírus chamado "*KoobFace*" ficou bastante famoso, ele era um *worm* que infectou usuários por meio de mídias sociais, como o Facebook. Uma vez situado no computador, ele podia coletar informações confidenciais e até números de cartão de crédito (KASPERSKY, 2017).

3.3 SPAM

Spams são mensagens indesejadas ou não solicitadas enviadas aos titulares de conta de e-mail ou mídia social. Na maioria das vezes, tais mensagens são maliciosas, embora alguns tenham procurado usá-la como estratégia de propaganda apenas. O uso de *spam* data desde quando redes de comunicação entraram em uso na Internet e eles cresceram com os avanços na comunicação nas

redes, não para aprimorá-lo, mas para contornar a comunicação bem-intencionada dos proprietários legais de contas. Pesquisas mostraram que, no primeiro semestre de 2013, o crescimento da mídia *spam* aumentou para 35% apenas na conta típica, salientando que uma das sete postagens sociais contém *spam* (NGUYEN, 2014). Realmente, o spam social é impulsionado usando meios diferentes. Isso inclui texto, imagem ou *links* com base em *URLs*. O *spam* social baseado em *URL* geralmente omite o texto, deixando apenas o *link* para o usuário clicar, apagando a atenção da vítima inocente.

Os *spams* sociais baseados em imagem aparecem como imagens atraentes ou anúncios com a potência de atrair na rede social determinados usuários para acessar seu conteúdo. Isso geralmente leva o usuário a outros computadores que baixam *malwares*, comprometendo sua confidencialidade.

3.4 XSS

O *Cross-Site-Scripting* (XSS) é um tipo de vulnerabilidade de segurança normalmente encontrada em aplicativos da *web* (OWASP, 2018). O XSS permite que atacantes injetem *scripts* do lado do cliente em páginas da *web* visualizadas por outros usuários e podem ser usados para ignorar o controle de acesso, como a política de mesma origem.

O impacto do XSS pode variar de um pequeno incômodo a um risco significativo de segurança cibernética, dependendo da sensibilidade dos dados manipulados pelo site vulnerável e da natureza de quaisquer atenuações implementadas.

Uma vez tendo sucesso com essa falha nas redes sociais, o atacante faz com que seu ato malicioso se hospede em servidores confiáveis, fazendo com que o ataque seja bem-sucedido.

3.5 CSRF

A *Cross-Site Request Forgery* (CSRF) é um ataque que força um usuário final a executar ações indesejadas em um aplicativo web no qual eles estão atualmente autenticados (OWASP, 2018). Os ataques CSRF visam especificamente solicitações de alteração de estado, não roubo de dados, pois o

invasor não tem como ver a resposta à solicitação forjada. Com uma pequena ajuda da engenharia social (como o envio de um *link* por e-mail ou até no *chat* privado das redes), um invasor pode induzir os usuários de um aplicativo da *web* a executar ações de sua escolha. Se a vítima for um usuário normal, um ataque CSRF bem-sucedido pode forçar o usuário a executar solicitações de alteração de estado, como transferência de fundos, alteração de endereço de e-mail e assim por diante. Se a vítima for uma conta administrativa, o CSRF poderá comprometer todo o aplicativo da *web*.

3.6 SQL INJECTIONS

Injeção SQL é uma abordagem técnica usada pelos atacantes para obter acesso a base de dados (OWASP, 2018). A mitigação desse ataque é deixada principalmente para os desenvolvedores do website. Conforme conclusão do relatório da Slow PC (2014), foi revelado que que o Facebook e o Twitter eram os sites que mais sofreram ataques SQL em comparação com os sites do governo americano.

3.7 ROUBO DE CREDENCIAIS

O roubo de identidade ocorre quando os invasores roubam as credenciais de outros usuários, identificando dados como perfil, foto, data e local de nascimento e, em seguida, utilize estas informações para criar outra conta. Essa nova conta é usada principalmente para fins de propósitos fraudulentos. Mali (2014) afirma que 12 milhões de pessoas foram vítimas de roubo de identidade e fraude em 2012, e a perda financeira deste ataque foi estimado em US $ 21 bilhões.

Conforme Florencio (2008), em seu artigo de título: O *phishing* como tragédia dos comuns (tradução livre), os ataques ocorrem onde o acesso tem como alvo os recursos que são difíceis de se regenerar. No capítulo a seguir, será aprofundado como estas credenciais são usadas para gerar um ataque mais especializado, que são chamados de ameaças persistentes avançadas.

4. APT - ADVANCED PERSISTENT THREAT

O *Advanced Persistent Threat (APT),* de acordo com Hoffman (2018), é um grande problema de *cybersecurity* que muitas organizações, grandes ou pequenas, poderão enfrentar eventualmente. Os ataques de APT típicos envolvem um ou mais *hackers* profissionais, pagos para invadir a rede de uma organização e roubar informações.

Ainda segundo Hoffman (2018), os *hackers* podem ficar na rede por um longo tempo antes de serem detectados, e seu propósito é obter dados proprietários, informações classificadas ou dados similares que podem ser explorados para lucro ou até mesmo usados para causar danos à segurança nacional.

Ao contrário de tipos de ataque, complementa Hoffman (2018), um ataque de APT é altamente sofisticado e muito bem planejado, ao contrário do ataque do tipo "*smash and grab*". Os *hackers* operam de maneira metódica, iniciando com o reconhecimento da vítima e são financiados por grupos criminosos bem estruturados, organizações militares ou agências governamentais.

4.1 O QUE É ADVANCED PERSISTENT THREAT?

Uma definição de APT, conforme Bejtlich (2010), *Advanced Persistent Threat*, traduzida para o português como "ameaça persistente avançada", foi cunhado pela Força Aérea dos Estados Unidos em 2006, pois precisavam de um termo não-classificado para se comunicar com colegas do mundo exterior. Os membros do Departamento de Defesa geralmente atribuem termos classificados para pessoas que atuam em um determinado tipo de ameaça, como não poderiam utilizar o termo classificado para comunicação com o pessoal não autorizado, decidiram criar um termo que serviria como um "apelido" ao respectivo termo classificado, muitas vezes utilizando somente sua sigla, APT. O termo APT costumava ser utilizado com mais frequência para se referir a grupos distintos que operam na região oriental da Ásia, porém também pode ser utilizado como um termo geral para outros grupos com as mesmas características destes.

Ainda segundo Bejtlich (2010), a maioria dos que combatem ativamente os ataques de APT descrevem o inimigo da seguinte forma:

> **“*Advanced***, ou avançada, significa que o inimigo pode operar de forma ampla nos equipamentos, podendo usar todo tipo de intrusão, desde a exploração conhecida de uma vulnerabilidade básica e comum como também podem avançar para a pesquisa de novas vulnerabilidades, até então desconhecidas, e desenvolver outras formas de exploração personalizadas, dependendo do alvo.
>
> ***Persistent***, ou persistente, significa que o inimigo é recrutado formalmente para a realização de uma missão. Não são invasores ocasionais, casuais ou oportunistas. Como uma unidade de inteligência, cumprem diretrizes para satisfazer as ordens recebidas dos superiores. Persistente não significa que o código malicioso precisa ser executado de forma constante nos equipamentos das vítimas, mas que se deve manter o nível de interação necessária, até que os objetivos do ataque sejam atingidos.
>
> ***Threat*****,** ou ameaça, significa que o inimigo possui uma organização, um financiamento e uma motivação para sua realização, não é simplesmente um código. Alguns falam sobre vários grupos que se organizam em formas de “equipes”, dedicadas à realização de diversas missões.”

Resumindo, APT seria um inimigo que realiza operações digitais ofensivas, conhecidas como operações de rede ou exploração de rede de computadores como base para o objetivo que se pretende alcançar. Uma característica de APT é manter algum grau de controle sobre a infraestrutura de informática de seu alvo, atuando persistentemente para preservar este controle, ou readquiri-lo, se necessário. Agentes de contra inteligência e analistas militares costuma utilizar o termo “agressivo” para enfatizar o grau de atuação dos grupos de APT que perseguem o objetivo contra seus alvos, sendo eles governamentais, militares ou mesmo grandes corporações privadas.

4.1.1 BUSINESS E-MAIL COMPROMISE

O *Business E-mail Compromise* (BEC) ou, em uma livre tradução, comprometimento de e-mail corporativo, de acordo com o FBI (2019), é uma fraude sofisticada cujo alvo são indivíduos ou empresas que realizam pagamentos por transferência eletrônica. O golpe geralmente é realizado quando o atacante compromete contas de e-mail comerciais legítimas, por meio da engenharia social ou através de técnicas de intrusão de computadores, para a realização de transferências não autorizadas de fundos. Porém a fraude nem sempre está vinculada a uma solicitação de transferência de fundos, podendo ser também utilizada para a obtenção de informações de identificação pessoal, ou salários e impostos dos funcionários FBI (2019).

O FBI (2019) também sugere algumas medidas de proteção: “Os funcionários deverão ser informados e estarem alertas quanto ao esquema. O treinamento deve incluir medidas reativas e estratégias de prevenção para o caso de serem vítimas.”

Dentre outras etapas, o FBI (2019) sugere que os funcionários deverão ser instruídos para:

- Utilizar canais secundários, ou dois fatores de autenticação, para a verificação de alterações de informações em sua conta.
- Verificar se os *links* dos e-mails recebidos realmente estão associados às empresas aos quais afirmam pertencer.
- Ficar atento quanto a *links* que possuem erros de ortografia no nome do domínio.
- Não fornecer credenciais ou informações de identificação pessoal em respostas de e-mails.
- Monitorar regularmente as contas pessoais em busca de irregularidades.
- Manter todos os *patches* de *software* e sistema atualizados.
- Verificar o endereço de e-mail utilizado para o envio, especialmente se estiver utilizando um dispositivo móvel ou portátil, para ter certeza de que o endereço de e-mail corresponda de fato ao remetente.
- Verificar se as configurações dos equipamentos dos funcionários estão habilitadas para permitir a visualização das extensões completas nos e-mails.

4.2 BEC COMO UMA DAS PRINCIPAIS FORMAS DE ATAQUES DO TIPO APT

De acordo com Rice (2018), o comprometimento de e-mail corporativo está em ascensão e custando às companhias bilhões de dólares, tanto que o *Internet Crime Center* do FBI, passou a considerá-lo um tipo único de crime, devido às suas similaridades e técnicas, e se distinguem de outras fraudes de e-mail nas etapas, tempo e esforço consumidos para elaborar a campanha criminosa. Estes passos se enquadram na estrutura utilizada pelas ameaças persistentes avançadas e isso é o que o torna perigoso.

Há anos já é conhecido o fato de que, por mais que uma companhia esteja protegida, os profissionais de segurança não podem garantir que a rede não será violada por adversários avançados RICE (2018).

Ataques de APT geralmente usam um vetor de e-mail para o envio de *softwares* ou *links* maliciosos em uma rede. Então, dependendo do valor do alvo, criam ou descobrem vulnerabilidades que possam garantir que o ataque passe despercebido pelos sistemas de proteção existentes, evitando o alerta ao time de segurança de rede RICE (2018).

Ainda segundo Rice (2018), ataques a muitas companhias utilizam uma combinação de engenharia social com *softwares* maliciosos.

4.3 FERRAMENTAS

Conforme Panetta (*Gartner Top 10 Security Projects for 2019)*, dentre as ferramentas mais utilizadas no mercado para prevenção ou atenuação de ataques de comprometimento de e-mail corporativo (BEC), podemos citar:

Trend Micro Advanced Threat Protection[5]: faz parte dos pacotes de soluções personalizadas da Trend Micro, e afirmam oferecer proteção na combinação de técnicas de defesa multigerações contra ataques direcionados, ameaças avançadas e *ransomware*, com a capacidade de detectar, analisar e responder aos ataques direcionados em tempo real. A Trend Micro afirma que os golpes de *business e-mail compromise* dependem de engenharia social, portanto podem ser evitados de uma forma mais eficiente se, além da ferramenta, for acompanhado de treinamento dos funcionários, para isso, incluem uma solução chamada *Phish Insight* que permite o envio de e-mails de *phishing* realistas aos seus usuários e, através do monitoramento de quem clicou nos *links* ou acessou o conteúdo do e-mail isca, identificar a necessidade em oferecer o treinamento para os que se apresentaram mais vulneráveis ou suscetíveis ao risco.

[5]"Advanced Threat Protection | High Detection ... - Trend Micro." https://www.trendmicro.com/en_in/business/products/network/advanced-threat-protection.html. Data de acesso: 21 jun.. 2020.

Gatefy Secure Email Gateway[6]: o fornecedor oferece um produto que possui diferentes ferramentas e mecanismos para proteger redes de e-mail contra todo tipo de ataque e ameaça, como por exemplo, *ransomware* e *phishing*. Dentre os recursos de proteção, uma citada é a *Content Disarm & Reconstruction*, que significa Desarmar e Reconstruir Conteúdo, que basicamente é desconstruir um arquivo, remover ou desarmar o conteúdo ativo, e reconstruir o arquivo higienizado, além de análises de *links* e detecção baseada em inteligência artificial. Ainda garantem desempenho e disponibilidade para seus aplicativos, por utilizarem uma arquitetura de micro serviço, que permite que diferentes aplicativos compartilhem um único sistema operacional e recursos do hospedeiro, mas que sejam executados de forma independente através de containers. Também informam que as organizações podem customizar a ferramenta, permitindo que controlem as informações que poderão ser compartilhadas pela rede de e-mail, através de filtros personalizados. Também implementam proteção adicional com o uso de antivírus e de anti-DDoS.

Microsoft Advanced Threat Protection[7]: este produto está vinculado ao Microsoft Office 365, e dentre os recursos oferecidos, pode-se citar a proteção e detecção de *links*, anexos maliciosos, controles de ameaças, investigação avançada de ameaças, dependendo do plano escolhido. Oferece inclusive a integração total com suas ferramentas, além da proteção do e-mail, permite a proteção de anexos no SharePoint, OneDrive e Teams, e proteção de *links* no Teams, além de simulação de ataques, controle e investigação de ameaças, dependendo do plano escolhido pela companhia.

As três ferramentas anteriormente apresentadas foram avaliadas no âmbito das suas características tecnológicas para reunir no quadro 1, seus variados recursos, plataformas de e-mail compatíveis, tipos de implementação e principais diferenciais[8].

---

[6] "O que é um Secure Email Gateway (SEG)? - Gatefy." 1 out.. 2019, https://gatefy.com/pt-br/postagem/o-que-e-um-secure-email-gateway-seg/. Data de acesso: 21 jun.. 2020.
[7] "Proteção Avançada contra Ameaças do Office 365 - Microsoft." https://www.microsoft.com/pt-br/microsoft-365/exchange/advance-threat-protection. Data de acesso: 21 jun 2020.
[8] Fontes: https://www.microsoft.com/pt-br/microsoft-365/exchange/advance-threat-protection/ https://www.trendmicro.com/pt_br/business/products/user-protection/sps/email-and-collaboration/cloud-app-security.html

	TREND MICRO Advanced Threat Protection	**GATEFY Secure Email Gateway**	**MICROSOFT Advanced Threat Protection**
Inteligência Artificial	Sim	Sim	Não
Detecção de URLs	Sim	Sim	Sim
Detecção de anexos	Não	Sim	Sim
Detecção de conteúdo	Sim	Sim	Sim
Detecção de remetentes	Sim	Sim	Sim
Plataformas compatíveis	Office 365 e G Suite	Office 365, Exchange, G Suite e Zimbra	Exchange e Office 365
Implementação	Nuvem	Nuvem, Híbrido, Virtual e *On-Premise*	Nuvem
Diferenciais	Treinamento para os funcionários	Alto desempenho e disponibilidade, regras e políticas customizáveis, defesa avançada e direcionada	Integração total com as ferramentas Windows

Quadro 1

Conforme elucidam Mitnick e Simon (2002), mesmo que sejam implementadas as tecnologias mais avançadas por uma empresa, ainda que os recursos financeiros fossem ilimitados, que os funcionários recebessem treinamento adequado sobre segurança e prevenção além de trancar todos os dados sensíveis antes de ir embora ou contratado guardas para proteger as instalações físicas. Mesmo assim, esta corporação continuará vulnerável.

Partindo deste pensamento e de todo contexto apresentado até aqui, concordando com o que dizem Mitnick e Simon (2002), as pessoas podem seguir cada uma das melhores práticas de segurança recomendadas pelos melhores especialistas, podem implementar cada produto de segurança recomendado e vigiar atentamente a configuração adequada do sistema e a aplicação das correções de segurança, mas provavelmente esses indivíduos ainda estarão completamente vulneráveis.

5. CONSIDERAÇÕES FINAIS

Após aprofundar os conceitos da psicologia e compreender a maneira que a mente humana absorve certas emoções e constrói sentimentos, foi descoberto que para o indivíduo é inerente suprir algumas necessidades básicas para que recebam aprovação de outrem ou sejam aceitos. Especificamente a partir daí, surgem naturalmente as vulnerabilidades que os engenheiros sociais, se utilizando dos princípios da retórica, podem explorar facilmente com intuito de manipular outros em benefício próprio.

A era da informação trouxe inúmeros benefícios ao homem, porém potencializou exponencialmente os riscos atrelados à engenharia social. Quando a maioria se depara com o termo “cibercriminosos”, tende a formar uma imagem estilizada de pessoas excluídas da sociedade e que ficam escondidas em uma sala escura ao cometerem seus delitos, acreditando que a meta destes, seja puramente contaminar tão quanto o maior número possível de alvos e equipamentos. Porém, ao investigar o tema com mais cautela fica claro: a verdade é bem diferente desta falácia. É revelado, que o agressor conhecido como *hacker* na cultura popular, tem muitas formas e faces. É um atacante, preparado, discreto e multifacetado, não sendo uma tarefa simples reconhecê-lo na multidão, ao contrário, é um processo delicado e demasiadamente árduo.

A combinação de tecnologia com os especialistas na arte de enganar, transformou o mundo e gerou impactos no método que é ímpar no cuidado com tais ameaças. Hoje, não mais analógicas e visíveis como outrora, mas sim, digitais e camufladas, praticamente invisíveis. Em síntese, o modelo dos seres humanos se relacionarem, trabalharem e viverem mudou drasticamente. Para quem viu o mundo antes desta metamorfose, em última instância, será confuso conseguir acompanhar devido abrupta velocidade no giro de cento e oitenta graus ocorrido. Como consequência, uma grande parcela dos que fazem parte deste grupo, tornaram-se o foco majoritário na mira dos criminosos, principalmente por ocuparem altos cargos de responsabilidade nas empresas e nem sempre, reconhecerem o perigo iminente à espreita. O produto resultante desta equação é justamente o ataque persistente avançado (APT). Por ser planejado de maneira meticulosa e com o objetivo de ser

habitualmente silencioso e eficaz, mesmo após atingir o equipamento que possui algum tipo de informação útil ou segredos valiosos, para suprimi-lo são necessárias ferramentas tão elaboradas quanto às técnicas empenhadas pelos invasores.

Diversas empresas investem em programas de conscientização e treinamento para disseminar uma cultura corporativa focada em segurança da informação. Por isso, é imperativo (e indispensável) que o tema também seja do interesse dos colaboradores da instituição como um todo. A razão para tal empenho se dá pela característica particular do APT, que combina técnicas variadas para chegar ao seu destino, utilizando constantemente pessoas da cadeia de confiança do alvo predominante. Logo, a multiplicidade dos controles mitigatórios é diretamente proporcional ao desafio na rastreabilidade dos riscos. Ainda que as ferramentas de mercado reúnam os mais recentes avanços no desenvolvimento de proteções adequadas para cumprir sua missão desafiadora, ao estudar suas particularidades, é notável que tais recursos venham num crescente movimento para tentar mitigar os ataques persistentes avançados.

O mote principal do presente trabalho foi compreender a eficácia de três softwares de companhias distintas: 1) Advanced Threat Protection da Trend Micro; 2) Secure Email Gateway da Gatefy; e 3) Advanced Threat Protection da Microsoft, que visam impedir o famigerado ataque conhecido como Business E-Mail Compromise (BEC), como falamos, um tipo especial de APT. Sendo destes o mais recomendável, segundo a análise apresentada, a ferramenta desenvolvida pela Gatefy, devido suas especificidades. Seus principais diferenciais são o alto desempenho e disponibilidade, suas regras e políticas customizáveis e sua defesa avançada e direcionada. Ela também dispõe de inteligência artificial, atende aos requisitos de detecção de remetentes, URL, anexo e conteúdo. Somados com sua implementação (a mais adaptável delas), uma vez que vai desde *on-premise*, virtual, híbrido até finalmente a opção na nuvem. Neste quesito, é importante ressaltar que as demais são comercializadas apenas na modalidade de implementação SaaS (Software as a Service), uma tendência do mercado de software, de oferecer produtos apenas *Cloud*. O Secure Email Gateway também se mostrou compatível com uma maior gama de serviços de e-mail (Office 365, Exchange, G-Suite e Zimbra) o que, em nossa opinião, culminou com sendo a melhor das três.

Entretanto, ao ponderar que os ataques de BEC do tipo APT são formados pela soma da experiência dos peritos em engenharia social e o conhecimento técnico especializado, concluímos que toda possível customização e aprimoramentos presentes nas ferramentas atuais, ainda não garantem um nível de proteção e excelência adequado para combater os diversificados tipos de comprometimento de e-mail corporativo, através dos ataques persistentes avançados. Portanto, a mitigação plena e definitiva precisará não apenas do auxílio dos recursos tecnológicos destes softwares, como também de políticas, treinamentos dos envolvidos e testes constantes. Haja visto que a escolha de acessar um site desconhecido, clicar em um endereço suspeito entre outros, depende em último caso de uma decisão particular e subjetiva de quem se torna alvo. Ou seja, ainda é necessário combinar diferentes esforços para atenuar o risco e alcançar um patamar mínimo de segurança da informação.

REFERÊNCIAS

ALVES, Cassio Bastos. Segurança da informação Vs. Engenharia Social como se proteger para não ser mais uma vítima. Disponível em: https://adm-portal.appspot.com.storage.googleapis.com/_assets/modules/academicos/academico_3641.pdf. Acesso em: 05 jun. 2020.

APPOLINÁRIO, F. **Metodologia da Ciência: filosofia e prática da pesquisa**. São Paulo: Cengage Learning, 2009.

ARISTÓTELES. **Arte Retórica e Arte Poética**. Introdução Goffredo Telles Junior. Tradução de Antônio Pinto de Carvalho. Rio de Janeiro: Ediouro - Tecnoprint, 1979.

ARISTÓTELES. **Retórica**. Manuel Alexandre Júnior, Paulo Farmhouse Alberto e Abel do Nascimento Pena. São Paulo: Folha de São Paulo, 2015.

BEC. (Business Email Compromise). **Trend Micro USA**, 2019. Disponível em: https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec). Acesso em: 10 set. 2019.

BEJTLICH, Richard. **What APT is (and what it isn't)**. Jul. 2010. Information Security Magazine. Disponível em: https://www.academia.edu/6842130/What_APT_Is. Acesso em 14 jun. 2020.

BULLAS, J. (2013). **5 Insights into the latest social media facts.** Disponível em: http://www.jeffbullas.com/2013/07/04/5-insights-into-the-latest-social-media-facts-figuresand-statistics/. Acesso em 21 jun. 2020.

C. Herley e D. Florencio. **Phishing as a Tragedy of the Commons**. NSPW 2008, Lake Tahoe, CA, 2008.

CIALDINI. R. **Influence: science and practice**. Allyn and Bacon, 2001.

CIAVATTA, Marina. We Talk to Physical Penetration and Social Engineering Expert, 2019.

FBI. **Public Service Announcement, Alert Number I-091019-PSA**. 10 set. 2019. Disponível em: https://www.ic3.gov/media/2019/190910.aspx. Acessado em 21 jun. 2020.

FERREIRA, L. A. **Leitura e persuasão: princípios de análise retórica**. São Paulo: Contexto, página 110, 2010.

GRANGER, S. **Social Engineering Fundamentals**, Part I: Hacker Tactics. SecurityFocus, 2001.

GUNATILAKA, D., **(2011). A survey of privacy and security issues in social networks**. Disponível em: http://www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.html. Acesso em 21 jun. 2020

Hackers Clothing - MyHackerTech, 2019. Disponível em: https://myhackertech.com/blogs/news/we-talk-to-physical-penetration-and-social-engineering-expert-marina-ciavatta. Acesso em: 19 out. 2019.

HOFFMAN, Susan. **Advanced Persistent Threats and How Your Organization Can Deter Them**. Disponível em: https://incyberdefense.com/featured/advanced-persistent-threats-deter/. Acesso em 20 jun. 2020.

KASPERSKY, **O que é o KoobFace?.** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-the-koobface-virus Acesso em 21 jun. 2020.

K. Marett, D. Biros, and M. Knode. Self-efficacy, **Training Effectiveness, and Deception Detection: A Longitudinal Study of Lie Detection Training.** Páginas 187–200, 2004.

K. Mitnick e W. Simon. **The Art of Deception: Controlling the Human Element of Security.** Wiley, 2002.

MALI, J. Disponível em: https://www.lifehack.org/articles/technology/identity-theft-through-social-networking-lessons-take-now.html. Acesso em 21 jun. 2020.

MARSTON, W. M. **Emotions of Normal People**. [S.l]: Routledge, 2013.

M. de A. MARCONI e E. M. LAKATOS. **Fundamentos de metodologia científica**. 6ª. ed. São Paulo: Atlas, 2009.

MYERS, D. G. **Introdução à psicologia**. Rio de Janeiro: LTC, 1999.

NELSON, R. **Methods of Hacking: Social Engineering**. 2008. Disponivel em: http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html. Acesso em 05 jan. 2020

NGUYEN, H., (2013). Research Report 2013 State of Social Media Spam, NextGate Publication, San Francisco. Disponivel em: http://nexgate.com/wpcontent/uploads/2013/09/Nexgate-2013-State-of-SocialMedia-Spam-Research-Report.pdf/. Acesso em 21 jun. 2020.

OWASP TOP 10, Disponível em: https://owasp.org/www-community/attacks/. Acesso em 21 jun. 2020.

PANETTA, K. **Gartner Top 10 Security Projects for 2019.** Smarter With Gartner, 2019. Disponível em: https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2019 . Acesso em: 10 set. 2019.

Pathos, Ethos e Logos:**a retórica de Aristóteles.** https://amenteemaravilhosa.com.br/pathos-ethos-e-logos/. Acesso em 16 mar. 2020.

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

PROVENZANO, F. **Falso coronel é preso após entrar na Base Aérea de São Paulo.** Extra Online, 2016. Disponível em: https://extra.globo.com/casos-de-policia/falso-coronel-preso-apos-entrar-na-base-aerea-de-sao-paulo-18739777.html. Acesso em 24 set. 2019.

QIN T. e BURGOON, J. **An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering.** Intelligence and Security Informatics, páginas 152–159, 2007.

SCHAWARTAU, W. Engenharia social: **pessoas ainda são elo mais fraco, diz especialista.** Instituto de Engenharia, 16 mar. 2010. Disponível em: https://www.institutodeengenharia.org.br/site/2010/05/25/engenharia-social-pessoas-ainda-sao-elo-mais-fraco-diz-especialista/. Acesso em: 10 set. 2019.

Slow PC. Disponível em: http://www.spamfighter.com/News-13034-HackersPrefer-SQL-Injection-Attack-Social-NetworksWebsites.htm. Acesso em 21 jun. 2020.

STASIUKOSIS, S. **Social Engineering, the USB Way**. 2006. Disponível em http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634. Acesso em 06 jun. 2020.

T. JAGATIC, N. JOHNSON, M. JAKOBSSON, e F. MENCZER. **Social phishing**. Communications of the ACM, 50(10):94–100, 2007.

TRUTA, F. **59% of people use the same password everywhere, poll finds.** Disponível em: https://hotforsecurity.bitdefender.com/blog/59-of-people-use-the-same-password-everywhere-poll-finds-19851.html. Acesso em 21 jun. 2020.

Vanheuangdy, V. (2010). **Security Threats of Web 2.0 and Social Networking Sites**, Disponível em: http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626+Security+Threats+of+Web+2+and+SNS+V+Vanheuangdy.pdf. Acesso em 21 jun. 2020.

WRIGHT, O. Hacking without Computers – An Introduction to Social Engineering. **Context Information Security**, 2019. Disponível em: https://www.contextis.com/en/blog/hacking-without-computers-an-introduction-to-social-engineering. Acesso em: 19 out. 2019.