INTERFACE TECNOLÓGICA

ENGENHARIA SOCIAL: um perigo oculto em simples técnicas

SOCIAL ENGINEERING: a danger hidden in simple techniques

Vinícius da Silva Geraldo – viniciusgeraldo96@hotmail.com
Fábio Bento Takeda – fabio.takeda1@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (FATEC) – SP – Brasil

RESUMO

A informação pode ser considerada como o maior bem de organizações, por isso há uma grande necessidade de protegê-la. Este trabalho tem por objetivo abordar e apresentar algumas técnicas de engenharia social, de forma que o público em geral possa conhecer atitudes reais do dia-a-dia, e assim, evitar se tornarem vítimas destas ações. A realização deste estudo baseou-se em um formulário eletrônico, o qual, foi disponibilizado de forma aberta via Internet para que as pessoas respondessem questões. A elaboração das questões foi baseada em agrupamentos das subáreas da engenharia social, o que por si só, já representa uma técnica de engenharia social. Os resultados da pesquisa demonstraram que mesmo com os trabalhos de engenheiros sociais, uma parcela da população está sujeita à fragilidade no processo de segurança. Sugere-se que trabalhos de conscientização dos usuários devem ser ampliados dentro e fora das organizações para uma conduta mais segura.

Palavras-chave: Engenharia Social. Prevenção de Ataques. Segurança da Informação.

ABSTRACT

Information is considered to be one of the largest assets of an organization, so there is a prominent need to protect it. This paper aims to address and present some social engineering techniques that the general public can use to avoid becoming a victim of such actions. This study was based on an electronic form that was made available through the internet for people to answer questions. These issues were based on clusters of the sub-areas of social engineering, which in turn already uses a social engineering technique. The results of the analysis show that even with the work of social engineers, a portion of the population may be fragile in the security process. It has been suggested that user awareness should be expanded within and outside organizations for safer conduct.

Keywords: Social Engineering. Prevention of Attacks. Information Security.

1 INTRODUÇÃO

O ativo mais importante de uma organização é a informação, por isso é necessário métodos para protegê-las de pessoas mal-intencionadas. Ela está exposta a uma enorme variedade de ameaças e vulnerabilidades e por isso existe uma grande preocupação com a segurança desses dados.

O termo “engenharia social” (em inglês *“social engineering”)* é a arte de manipular pessoas a fim de obter as informações necessárias para realização de diferentes técnicas de ataque, como por exemplo, uma simples conversa. Com base nas abordagens de Mitnick e Simon (1963) e Mann (2011), pode-se definir a engenharia social como métodos de influenciar ou persuadir pessoas com o intuito de convencê-las a fornecer informações sigilosas de uma organização ou pessoal.

De acordo com Mitnick (2004), o engenheiro social pode ser definido como uma pessoa que pode utilizar um conjunto de técnicas para a manipulação da confiança de outras pessoas para ter acesso às informações privadas. É possível também, por meio das poucas informações que ele tem acesso, montar um plano sobre o alvo e com informações que ele acha irrelevantes, dão ao engenheiro a possibilidade de prejudicá-lo empresarialmente, socialmente, financeiramente ou psicologicamente.

É importante ressaltar que este tipo de técnica pode se apresentar sob diversas formas e estende-se a população em geral. Um exemplo que é noticiado com frequência pela mídia é o processo de falso sequestro, quando uma pessoa, ao se deparar com uma ligação de uma pessoa desesperada, já informa o nome de uma pessoa conhecida, o qual colabora para o sucesso da ação.

Atualmente, ainda não é a cultura das organizações investirem em treinamento e na conscientização dos funcionários para este tipo de ação. Segundo Mann (2011), a maioria das empresas procura se concentrar nas novas ferramentas de proteção tecnológicas, como por exemplo, firewalls, biometria etc., mas não é o suficiente.

A metodologia empregada neste trabalho é a pesquisa bibliográfica, que foi realizada através de livros, artigos e revistas, que aborda a engenharia social. Com isso, buscando entender melhor seus conceitos e como ela é utilizada pelos engenheiros.

Este trabalho tem por objetivo abordar e apresentar algumas técnicas de engenharia social, de forma que o público em geral possa conhecer atitudes reais do dia-a-dia, e assim, evitar se tornarem vítimas destas ações.

O presente estudo será iniciado apresentado conceitos sobre a engenharia social, uma análise sobre suas ameaças e alguns tipos de ataques que podem ser utilizados para obter informações, bem como despertar o interesse tanto das pessoas e organizações a conscientizar sobre os perigos destes ataques. Também demonstrará os resultados obtidos a partir de um questionário eletrônico divulgado por meio de uma rede social.

2 ENGENHARIA SOCIAL

A engenharia social pode ser definida como conjunto de métodos e técnicas com o objetivo de obter informações sigilosas através de técnicas investigativas, psicológicas e de enganação. Para isso, o engenheiro se faz passar por outra pessoa, assumindo outra personalidade, com o objetivo de conseguir informações através de contato com parentes e amigos da vítima e outras técnicas para conseguir informação sigilosa (PARODI, 2008; HINTZBERGEN *et al*., 2018).

O ser humano é uma peça fundamental quando assunto aborda a segurança da informação. Ele se relaciona diretamente, visto que ele está envolvido com os processos, de modo que cada pessoa é uma peça chave para manter essa informação segura (FONSECA, 2017).

Soares (2001, apud MOTA, 2009, p. 13) adverte que a engenharia social compreende a inaptidão das pessoas de ficarem atualizadas com questões pertinentes relacionadas à tecnologia da informação, além de não saberem o real valor das informações que a possuem e não terem a preocupação em protegê-las de forma consciente.

Para Henriques (2016), a engenharia social envolve a exploração do senso comum das pessoas para adquirir informações preciosas de uma organização (como senhas, logins, informações organizacionais) através de funcionários despreparados para este tipo de situação.

2.1 TIPOS DE ATAQUES

Com a disseminação da Internet conectando tudo, tem-se uma situação sem precedentes no acesso às informações sensíveis das organizações e de governos ao redor do mundo. Esses acessos deixaram de ser simples jogos de hackers, que competiam entre si para ver quem conseguia invadir primeiro um servidor, para ser uma atividade orquestrada por grandes empresas e governos, com o objetivo de espionagem industrial e armas de destruição em massa (CARVALHO, 2014).

A Engenharia Social tornou-se um dos maiores riscos de segurança de empresas. As técnicas utilizadas estão cada vez mais sofisticadas e na maioria das vezes aproveitam-se das vulnerabilidades humanas que não se dão conta de que estão sofrendo um ataque (FONSECA, 2017). Existe uma grande gama de técnicas de invasão baseada em engenharia social. A seguir, são apresentadas algumas das técnicas analisadas neste trabalho.

2.1.1 INTERNET E REDES SOCIAIS

Com o uso da internet e as redes sociais entre pessoas, uma nova forma do engenheiro social garimpar informações foi aberta.O engenheiro pode começar a analisar sua vítima buscando informações na Internet, consultando o site da empresa na qual trabalha, nas redes sociais para conhecer melhor suas amizades, verificando perfil entre outros, buscando o máximo de informação que conseguir (JUNIOR, 2011).

2.1.2 CONTATO TELEFÔNICO

Após o processo inicial de coleta de informações sobre o alvo, o invasor poderá se passar por um funcionário terceiro ou fornecedor, o qual, através de um contato telefônico, poderá tentar extrair mais informações, explorando a vulnerabilidade de funcionários sem um treinamento coerente, auxiliando-o de forma involuntária no processo que poderá culminar em uma invasão (MAULAIS, 2016).

2.1.3 PHISHING

O phishing pode ser considerado como uma das técnicas mais utilizadas para conseguir uma determinada informação. O Phishing nada mais é que e-mails falsos que são manipulados e enviados para pessoas e organizações, com o objetivo de fazer com que o usuário aceite o mesmo e realize as operações que são solicitadas. Geralmente os casos mais comuns, são e-mails recebidos por bancos ou lojas, inventando uma história para que o usuário caia na isca. A maioria dos Phishing possuem algum anexo ou link dentro do e-mail que direciona o usuário a uma armadilha na qual ele deseja (MAULAIS, 2016).

2.1.4 ABORDAGEM PESSOAL

Está técnica é aplicada quando o invasor realiza uma visita na empresa na qual pretende atacar se passando por outra pessoa, seja funcionário, fornecedor ou amigo de alguma pessoa que exerce um cargo importante na empresa, utilizando suas técnicas de persuasão e falta de preparo do funcionário. Ele consegue sem dificuldade, convencer um segurança ou uma

secretária para liberar acesso ao servidor ou algum lugar que ele encontre informações que sejam valiosas (MAULAIS, 2016).

2.1.5 FALHAS HUMANAS

O elo mais fraco da segurança da informação está nas pessoas, no qual elas são as peças chave para se obter uma determinada informação. Com isso, os engenheiros sociais exploram as vulnerabilidades das pessoas como confiança, medo, curiosidade, ingenuidade, entre outros. Através de técnicas de persuasão, eles conseguem extrair informações das pessoas, sem ao menos saber que estão sendo vítima de um ataque de engenharia social (FONSECA, 2017).

3 PROCEDIMENTOS METODOLÓGICOS

Em complemento as atividades de revisão bibliográfica, optou-se por realizar uma atividade de campo, utilizando um formulário eletrônico com 19 (dezenove) questões, as quais, foram elaboradas para explorar situações comportamentais para a representação de parte da engenharia social. As questões elaboradas foram relacionadas a alguns tipos de ataques da engenharia social.

O formulário eletrônico online foi disponibilizado por meio de uma rede social, tentando atrair pessoas de diferentes classes sociais, atividades dentro e fora da área e com diferentes faixas etárias. Os resultados obtidos com o formulário foram sumarizados e apresentados na próxima seção.

4 RESULTADOS E DISCUSSÕES

A aplicação do questionário culminou em um conjunto de 132 (cento e trinta e duas) amostras válidas, as quais representam os elementos de análise deste trabalho. As análises iniciaram-se pelo agrupamento por tipo de ataque previamente selecionado conforme pode ser observado na Tabela 1.

Tabela 1 – Agrupamento das perguntas com base nos tipos de ataque.

Perguntas por Tipos de Ataque	Sim	Não	Não sei informar
Falhas Humanas			

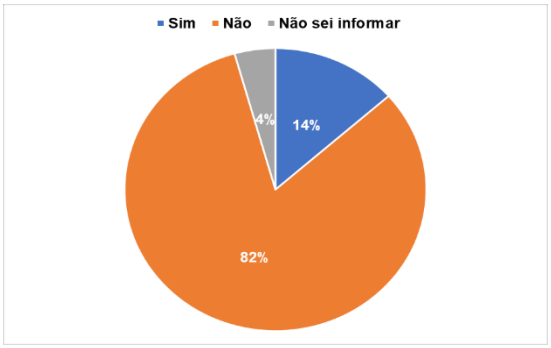
1 - A senha que você utiliza no seu local de trabalho para acessar as informações da empresa, você compartilha com outros funcionários?	8%	90%	2%
2 - Suas senhas pessoais são iguais às que você utiliza no trabalho?	12%	81%	7%
3 - Você costuma passar qualquer tipo de informações do seu local de trabalho para outras pessoas?	16%	80%	4%
4 - Você não utiliza as mesmas senhas para todas as suas contas?	19%	79%	2%
Contato Telefônico			
5 - Você costuma passar dados pessoais por telefone?	4%	85%	11%
6 - Geralmente esses números pedem informações pessoais ou alguma informação do seu local de trabalho?	38%	48%	14%
7 - Você costuma receber ligações de números que você não conhece?	84%	15%	1%
Internet e Redes Sociais			
8 - Você costuma postar fotos com seus colegas de trabalho nas redes sociais?	30%	55%	15%
9 - Você geralmente responde pessoas que te chamam no bate-papo para conversar, mesmo não conhecendo elas?	36%	63%	1%
10 - Nos perfis de suas redes sociais, você costuma colocar qual empresa você trabalha e qual o cargo que exerce?	54%	45%	1%
11 - No seu local de trabalho, você tem acesso as redes sociais (Facebook, Instagram, Twitter)?	69%	29%	2%
12 - É possível achar informações sobre sua empresa na Internet?	71%	20%	9%
Phishing			
13 – Geralmente, os e-mails que você recebe, você assinou eles para receber?	34%	57%	9%
14 - Alguma vez você já baixou algum arquivo de um e-mail que você recebeu sem perceber?	35%	60%	5%
15 - Você já recebeu algum e-mail pedindo para você passar dados pessoais, sendo que você não sabia qual a origem desse e-mail?	58%	38%	4%
16 - Você costuma receber e-mails de instituições financeiras e lojas?	88%	11%	1%
Abordagem Pessoal			
17 - Você costuma frequentar algum barzinho, academia ou qualquer outra coisa depois do trabalho?	42%	46%	12%
18 - Você gosta de conversar sobre o seu trabalho com seus amigos ou até mesmo pessoas que você não conhece?	46%	27%	27%
19 - Você é uma pessoa fácil de fazer amizade?	84%	10%	6%

Fonte: Os Autores (2019)

Os resultados obtidos serão apresentados baseando-se no item de resposta “Sim”, o qual foi o item de interesse nas respostas obtidas.

Após o agrupamento dos dados, foram gerados gráficos sumarizados com o conjunto de dados do agrupamento baseado em falhas humanas (**Erro! Fonte de referência não encontrada.**).

Figura 1 – Sumarização das respostas obtidas a partir de respostas que poderiam caracterizar ataques baseados em Falhas Humanas.



Fonte: Os Autores (2019)

Os resultados obtidos com a análise de falhas humanas (**Erro! Fonte de referência não encontrada.**) demonstram que esta ação não apresentou uma possibilidade de sucesso para um determinado invasor. Para Silva (2013), através da formação e da conscientização de pessoas e da implementação de normas, será possível amenizar falhas humanas e aumentar o nível de segurança da organização.

Vale ressaltar que, neste caso, o fato de manter as senhas pessoais e as profissionais diferentes só contribui para que haja uma certa dificuldade no acesso, pois, geralmente, muitas pessoas não têm tanto conhecimento na segurança de seus dados e podem ser submetidas a outras formas de ataques.

Outra forma de ataque é um simples contato telefônico. Baseando-se neste ataque, são apresentados os resultados obtidos na Figura 2.

Na Figura 2 nota-se que o número de respostas com valor “não” apresentou um maior valor percentual. Entretanto, se observar a quantidade de pessoas que responderam “não sei” em conjunto com o percentual das respostas “sim”, sugerem que o número de pessoas a cair neste tipo de ataque torna-se significativo.

Figura 2 – Sumarização das respostas obtidas a partir de respostas que poderiam caracterizar ataques baseados em Contato Telefônico.

Fonte: Os Autores (2019)

Recentemente, invasores utilizam esses meios para fazer vítimas, se passando por alguma pessoa e assim colocando seu plano em prática para enganar o alvo.

Ataques por telefone são comuns no dia-a-dia. Com informações simples sobre a vítima, como nomes, endereços, documentos, etc, é possível extrais mais informações importantes ou, por exemplo, se passar como um gerente de alguma empresa e pedir para a secretária fazer uma transferência de valores para uma determinada conta, sem que a vítima perceba que ela está sofrendo um ataque de engenharia social.

Para Fonseca (2017), o telefone é um dos meios mais utilizados pelos engenheiros, o uso dessa técnica oferece vantagens como a ocultação do número, anonimato e permite atuar em distância, o que dificulta encontrar o engenheiro.

Atualmente, obter informações de qualquer pessoa ou de uma determinada empresa tornou-se uma tarefa fácil na Internet. Milhares de pessoas acessam as redes sociais, as quais se transformaram em um instrumento rápido e de fácil coleta de informações. Os resultados obtidos na análise em técnicas de Internet e redes sociais são apresentados na Figura 3.

Figura 3 - Sumarização das respostas obtidas a partir de respostas que poderiam caracterizar ataques baseados em Internet e Redes Sociais.

Fonte: Os Autores (2019)

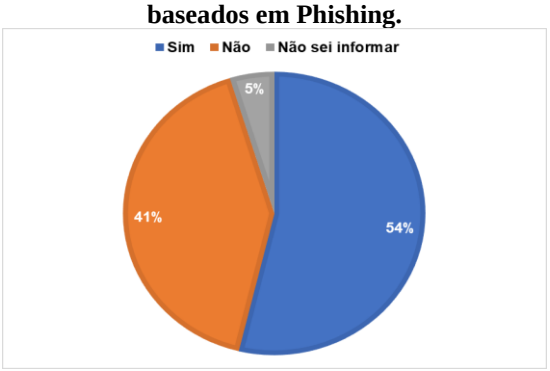
Nesta análise, foram realizados questionamentos sobre algumas informações que podem ser configuradas em redes sociais. A questão é que, os autores deste trabalho reconhecem a importância das redes sociais no e-marketing, entretanto, a disponibilização de determinadas informações pode indicar graus de afinidades entre pessoas, sobre assuntos de interesse, locais que frequentam com regularidade, horários de funcionamento da empresa etc.

Muitas pessoas, por esquecer dos detalhes que foram apresentados, compartilham estas informações, colocando em risco as empresas ou elas próprias, conforme foi observado na maioria das respostas obtidas (Figura 3).

Segundo Cortela (2013), quase todo internauta tem uma ou mais contas em redes sociais que possuem informações que poder ser críticas para um engenheiro tanto para criar um e-mail falso para enganar a vítima ou montar quadros útil para ataques mais convergentes.

Conforme mencionado anteriormente, ataques baseados em phishing são os mais comuns e a Figura 4 representa uma forma simples de extração de informação.

Figura 4 - Sumarização das respostas obtidas a partir de respostas que poderiam caracterizar ataques baseados em Phishing.



Fonte: Os Autores (2019)

Muitas pessoas são bombardeadas com vários e-mails de lojas, instituições financeiras, entre outros, só que nem sempre são confiáveis. Cada vez mais, torna-se impossível que os usuários lembrem de todos os lugares onde realizaram cadastros para receber e-mails.

Pessoas que costumam receber vários e-mails, às vezes acabam não se atentando a detalhes como ver quem é o emitente, o que ele está pedindo, se já ouviu falar dessa empresa e se está mandando acessar algum link ou baixar um arquivo.

O phishing é um golpe de e-mail direcionado com o objetivo de obter acesso a informações valiosas, com a intenção de furtar dados por exemplo financeiro, segredos comerciais e outros dados confidenciais de valor (MAULAIS, 2016).

Geralmente, são enviados e-mails falsos se passando por alguma loja, banco ou até mesmo alguma coisa relacionada a empresa na qual trabalha, pedindo para passar alguma informação importante ou até mesmo para baixar algum arquivo no seu computador ou acessar um link, iludindo o alvo a executar determinadas ações para conseguir informações sem que ela perceba. Com isso, mais da metade das pessoas que participaram da pesquisa poderia se submeter a estas atividades que poderiam de alguma forma, colocar em risco tanto a segurança

das informações pessoais de uma pessoa ou de uma organização, assim caindo em mãos erradas e prejudicando as vítimas.

A última técnica avaliada é associada à abordagem pessoal. Os resultados obtidos mostram ser o ataque de maior probabilidade de sucesso entre todas as estudas (Figura 5).

Figura 5 - Sumarização das respostas obtidas a partir de respostas que poderiam caracterizar ataques baseados em Abordagem Pessoal.

Fonte: Os Autores (2019)

Muitas pessoas acreditam que ter habilidades de fácil amizade pode ser considerada mais uma virtude do que algo ruim. De certa forma seria, entretanto em alguns casos, é possível que ao redor tenham pessoas que exploram estas características para se aproximar e extrair mais informações.

O problema da engenharia social é difícil de ser resolvido porque não está agregado ao código de programação ou hardware de computadores e sim nas falhas inerentes no comportamento de pessoas que podem ser exploradas pelos engenheiros (MITNICK, 2004).

Pessoas com esse tipo de comportamento acabam se tornando alvo de uma abordagem pessoal, no qual o agente se passando por outra pessoa e com suas técnicas de persuasão, começa a fazer perguntas sobre a empresa na qual trabalha ou até mesmo perguntas pessoais, com o intuito de extrair qualquer tipo de informação que possa ser utilizado para prejudicá-la.

5 CONCLUSÃO

Neste trabalho foram apresentados resultados que demonstraram que a maior parte da população analisada seria suscetível as técnicas de engenharia social. Este resultado ilustra a importância e o alto grau de comprometimento que estas ações possam de alguma forma, comprometer a segurança de pessoas e corporações.

Acredita-se que as respostas obtidas com os resultados “não sei informar” possam ampliar as chances de ataques, aumentando os resultados positivos deste trabalho, uma vez que, um fator de sucesso para um ataque de engenharia social é justamente a ignorância de ações ou comportamentos.

Existem vários relatos que relacionam os incidentes envolvendo a segurança da informação e em sua grande maioria, podem estar ligados ao fator humano. Ações de conscientização de pessoas são fundamentais para que corporações possam reduzir riscos e vulnerabilidades exploradas pela engenharia social.

Sugere-se a criação de uma rotina de palestras para conscientização deste tema com regularidade, para que membros da empresa possam identificar um ataque desta natureza, evitando que sejam submetidos a estas armadilhas.

REFERÊNCIAS

CARVALHO, Savio. Marcelo. **Transformação e Mudança:** 100 mini papers. São Paulo: Arbeit Factory Editora e Comunicação, 2014.

CORTELA, João José Corrêa. **Engenharia Social Aplicada ao Facebook.** 2013. Trabalho de conclusão de curso (Graduação em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2013.

FONSECA, Marcelo. **Engenharia Social:** conscientizando o elo mais fraco da segurança da informação. 2017. Trabalho de conclusão de curso (Pós-Graduação em Especialização em Inteligência em Segurança Pública) - Universidade do Sul de Santa Catarina, Brasília, 2017.

HADNAGY, Christopher**. Social engineering:** the art of human hacking. Indianapolis: Wiley Publishing, 2011.

HENRIQUES, Francisco de Assis Fialho. **A influência da Engenharia Social no fator humano das organizações.** 2016. Dissertação (Pós-Graduação em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2016.

HINTZBERGEN, J.; SMULDERS, A.; HINTZBERGEN, K.; BAARS, H. **Fundamentos de Segurança da Informação:** com base na iso 27001 e na iso 27002. Tradução: Alan de Sá. Rio de Janeiro: Brasport, 2018.

HODNIK, Carlos Eduardo. **Engenharia Social:** uma análise de ameaças e cuidados no mundo corporativo. 2017. Trabalho de conclusão de curso (Pós-Graduação em Segurança da Informação) - Universidade Estácio de Sá, Ribeirão Preto, 2017.

JUNIOR, Reinaldo Leopoldino Cavalcante. **Engenharia social nas redes sociais.** 2011. Trabalho de conclusão de curso (Monografia em Especialização em Desenvolvimento de Sistemas para Web) - Universidade Estadual de Maringá, Maringá, 2011.

MANN, Lan. **Engenharia Social**: séries prevenção de fraudes. São Paulo: Blucher, 2011.

MAULAIS, Claudio Nunes dos Santos. **Engenharia Social:** técnicas e estratégias de defesa em ambientes virtuais vulneráveis. 2016. Projeto de Pesquisa (Mestrado em Sistema de Informação e Gestão de Conhecimento) – Universidade Fumec, Belo Horizonte, 2016.

MITNICK, D. K. **A Arte de Enganar.** 1. ed. São Paulo: Pearson, 2004.

MITNICK, D. K.; SIMON, L. W. **Mitnick A arte de enganar. Ataques de Hackers:** controlando o fator humano na segurança da informação. Tradução: Kátia Aparecida Roque. São Paulo: Pearson, 1963.

MOTA, Felipe Antunes. **Engenharia Social.** 2009. Trabalho de conclusão de curso (Pós-Graduação como Requisito Parcial para Obtenção do Grau) - Universidade Candido Mendes, Rio de Janeiro, 2009.

PARODI, Lorenzo. **Manual das fraudes.** Rio de Janeiro: Brasport, 2008.

SILVA, Francisco José Albino Faria Castro e. **Classificação Taxonômicas dos Ataques de Engenharia Social.** 2013. Dissertação (Mestrado em Segurança dos Sistemas de Informação) – Universidade Católica Portuguesa Faculdade de Engenharia, Porto, 2013.