A Engenharia Social como ferramenta de obtenção não autorizada de dados de terceiros para a utilização no meio virtual.

Resumo. *A utilização da internet e dos meios virtuais como ferramentas de trabalho, entretenimento e aprendizado vêm crescendo desde o advento da internet. Com isso, milhares de informações pessoais ficam armazenadas em bancos de dados, cache, cookies, etc. Tendo em vista esse crescimento no meio virtual e o armazenamento de tantas informações, surgiram várias práticas criminosas com a intenção de obter tais dados de forma não autorizada para o uso em diversas finalidades. Através de eventos, fatos empíricos, estudos de caso e revisões bibliográficas pudemos desenvolver esse artigo e mostrar o quão perigosa pode ser a engenharia social, e o quão eficaz ela é na voz de alguém que domina a arte da persuasão.*

Abstract. *The use of the internet and virtual media as tools of work, entertainment and learning come growing since the advent of the internet. With that, thousands of personal information are stored in databases, cache, cookies, etc. In view of this growth in the virtual environment and storage of so much information, urgiram various criminal practices with the intent of obtaining such data in a way not authorized for use in a variety of purposes. Through events, empirical facts, case studies and bibliographical reviews we were able to develop this article, and show how dangerous can be social engineering, and how effective it is in the voice of someone who mastered the art of persuasion.*

1. Introdução

Atualmente a engenharia social vem ganhando um espaço cada vez maior desde a sua origem. Com isso vários escritores e estudiosos vêm investindo seu tempo no estudo dessa prática. No âmbito da segurança da informação, a engenharia social, pode ser uma prática executada ou não através de um sistema computacional, ou seja, ela não necessita de vírus ou exploits para obter as informações-alvo necessárias para que sejam feitas as invasões.

O *cracker* (pessoa com conhecimento avançado ou não em informática que utiliza programas maliciosos para cometer delitos) Kevin Mitnick escreveu em seu livro "A arte de enganar" (2001) que "a verdade é que não existe uma tecnologia no mundo que evite o ataque de um Engenheiro Social". Mesmo com o passar dos anos, essa definição de Mitinick permanece verídica, já que a engenharia social ataca diretamente o elo mais fraco de qualquer sistema de segurança avançado, que é o ser humano.

Frank William Abagnale é até hoje um dos engenheiros sociais mais conhecidos. Durante 5 anos na década de 1960 ele falsificou cheques nos Estados Unidos. Sua história de vida foi inspiração para o filme "Prenda-me se for capaz". Ele usava várias técnicas para conseguir cometer seus crimes, entre elas, ele imprimia seus próprios

cheques de forma quase perfeita, usando-os e enganando os bancos para liberar o dinheiro na troca desses cheques.

Frank Abagnale é apenas um exemplo de como a persuasão pode ser uma arma eficaz e prática para o roubo de dados e informações. De forma simples e fácil ele enganava gerentes e caixas de banco para conseguir efetuar transações com cheques falsos e sem fundo, empresas de aviação, se passando por piloto ou copiloto, escolas, se passando por professor e até mesmo hospitais quando se passava por médicos.

Por fim, o engenheiro social tem como objetivo principal ganhar a confiança das suas vítimas e a partir desse momento obter, de forma não autorizada, acesso a dados importantes. Dessa forma, ele consegue entrar em várias plataformas, ou simplesmente guarda esses dados para serem usados no futuro, como em compras ou cadastros. Sendo assim, o engenheiro social comete vários crimes e passa despercebido.

2. Trabalhos Relacionados

3. Metodologia

Para a criação deste artigo e aprofundamento na área de estudo escolhida, uma revisão bibliográfica foi feita em alguns periódicos online (como o CAPES e a plataforma SciELO). Após a compreensão de como a engenharia social é aplicada e como o engenheiro age, uma pesquisa em forma de formulário foi feita do período de 27/11/18 à 30/11/18 através do sistema *Google Forms*. Um total de seis perguntas foram feitas e veiculadas através de redes sociais (*Facebook* e *Whatsapp*) com o objetivo de coletar dados que nos permitissem analisar como algumas pessoas agem quando são submetidas a perguntas pessoais por pessoas conhecidas e desconhecidas. As perguntas presentes no questionário foram as seguintes:

Número	Conteúdo
1	Você já havia ouvido o termo "Engenharia social" antes?
2	Você já foi vítima de roubo de dados ou informações no meio virtual? (Como senhas bancárias, dados de cartão de crédito ou débito, ou informações pessoais como cpf, rg, data de nascimento, etc)?
3	Alguma vez você percebeu que alguém estava interessado de mais na sua vida pessoal ou em informações como nome de mãe/pai, data de aniversário, nome de animal de estimação ou algo similar?
4	Você já informou dados pessoais através da internet, ou comunicação pessoal e verbal ou através de outro meio de comunicação?

5	Alguma vez após uma conversa com alguém em um meio de comunicação, você sofreu algum crime cibernético ou teve acesso indevido de seus dados por terceiros (ações como distribuição de fotos íntimas, roubo de senha de instagram, facebook ou outra rede social)?
6	Você já recebeu alguma ligação onde a pessoa do outro lado da linha pedia suas informações pessoais ou já recebeu uma ligação onde afirmaram estar com alguém de sua família sequestrado?

Tabela 1. Descrição das perguntas do questionário.

Após esse questionário, uma análise foi feita em cima das respostas obtidas. Posteriormente, mais um questionário foi feito e direcionado apenas para os que responderam "sim" no primeiro, contendo perguntas diretas que deveriam ser respondidas em forma de texto em pequenos parágrafos. Esse outro questionário teve por objetivo saber como de fato as pessoas que já foram vítimas de roubos de informações agiram após serem vítimas ou perceberem que poderiam ser vítimas fáceis por terem dado informações importantes que deveriam ser sigilosas.

4. Resultados e Discussão

Antes do primeiro questionário ser respondido, uma breve explicação sobre a engenharia social era dada aos respondentes, para que assim pudessem compreender e responder de forma correta. A pesquisa teve um total de 44 participantes. A primeira pergunta pode ser vista figura 1, abaixo, junto com o percentual.

Figura 1. Respostas obtidas na primeira questão.

Como pode ser visto no gráfico presente na Figura 1, a maior parte das pessoas não conheciam o termo, isto é, 59,1% dos que responderam ao questionário (26 pessoas) nunca haviam ouvido falar em engenharia social antes, enquanto 40,9% (18 pessoas), sim. Percebe-se que a maioria das pessoas não conhecem ou nunca ouviram falar sobre "engenharia social". O segundo questionamento a ser feito, gerou um gráfico pizza. O gráfico percentual das pessoas que já foram vítimas ou não, pode ser vista na Figura 2, a seguir:

Figura 2. Segunda questão do primeiro questionamento.

Como pode ser visto no gráfico pizza presente na Figura 2, a maioria dos que responderam a pesquisa nunca tiveram seus dados roubados, ou seja, 65,9% (29 pessoas) nunca foram vítimas de roubos de informações, enquanto 34,1% (15 pessoas), foi. É preocupante ver que em uma pesquisa pequena com apenas 44 participantes, 15 já foram vítimas de roubo de dados importantes, o que faz crer que em uma pesquisa de

grande escala, o número de vítimas aumenta de forma diretamente proporcional ao número de participantes.

No segundo questionário feito, enviamos uma pergunta para todos os que responderam “sim” na pergunta presente na figura 2. A pergunta era facultativa, todavia, todos responderam. A questão foi a seguinte: “Se a resposta da segunda pergunta do primeiro questionário foi "sim", pode citar o que aconteceu (quais dados foram roubados) ?”. Muitas respostas foram dadas para essa pergunta. Selecionamos três dessas respostas para mostrar, as que foram consideradas mais completas e de maior impacto. Essas respostas podem ser vistas nas figura 3, abaixo:

5. Conclusão

Com todos os estudos de caso feitos, bem como revisões bibliográficas e análises empíricas nossas e de outras pessoas, podemos concluir que a engenharia social é uma ferramenta altamente eficaz quando executada por alguém que tem o dom da palavra e da persuasão. Sendo assim, o fator humano presente em qualquer sistema que seja, ainda é o elo mais fraco, e através dele pode-se obter sem muito esforço certas informações valiosas , e assim tornar-se facilmente vítima da engenharia social.

Referências

ASSIS, Francisco de. A influência da Engenharia Social no fator humano das organizações. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/25353/1/DISSERTA%C3%87%C3%83O%20Francisco%20de%20Assis%20Fialho%20Henriques.pdf>. Acesso em: 26 nov. 2018.

BRANDÃO, Cristiane Rodrigues.ENGENHARIA SOCIAL: UMA ANÁLISE DE AMEAÇAS E CUIDADOS AOS FUNCIONÁRIOS DAS AGÊNCIAS BANCÁRIAS DE SANTARÉM E ITAITUBA – PARÁ. Disponível em: <https://www.researchgate.net/publication/319551455_ENGENHARIA_SOCIAL_UMA_ANALISE_DE_AMEACAS_E_CUIDADOS_AOS_FUNCIONARIOS_DAS_AGENCIAS_BANCARIAS_DE_SANTAREM_E_ITAITUBA_-_PARA>. Acesso em: 30 nov. 2018.

DESCONHECIDO. SEGURANÇA DA INFORMAÇÃO VS. ENGENHARIA SOCIAL - COMO SE PROTEGER PARA NÃO SER MAIS UMA VÍTIMA. Disponível em:

<https://monografias.brasilescola.uol.com.br/computacao/segurancainformacao-vs-engenharia-social-como-se-proteger.htm>. Acesso em: 27 nov. 2018.

NUNES, ClÁudio. ENGENHARIA SOCIAL: TÉCNICAS E ESTRATÉGIAS DE DEFESA EM AMBIENTES VIRTUAIS VULNERÁVEIS. Disponível em: <http://www.fumec.br/revistas/sigc/article/viewFile/3733/2031>. Acesso em: 25 nov. 2018.

SANTOS, Rafael Cardoso dos. Engenharia social: atacando o elo mais fraco. Disponível em: <http://mauriciolyra.pro.br/site/wp-content/uploads/2015/12/09-Artigo-Engenharia-social.pdf>. Acesso em: 27 nov. 2018.