UNIVERSIDADE DO SUL DE SANTA CATARINA
MARCELO FONSECA

ENGENHARIA SOCIAL: CONSCIENTIZANDO O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO

BRASÍLIA
2017

MARCELO FONSECA

ENGENHARIA SOCIAL: CONSCIENTIZANDO O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO

Monografia apresentada ao Curso de Pós-Graduação *Lato Sensu* em Especialização em Inteligência de Segurança Pública, da Universidade do Sul de Santa Catarina, como requisito à obtenção do título de Especialista em Inteligência de Segurança Pública.

Orientação: Prof. Camel André de Godoy Farah, Dr.

BRASÍLIA
2017

MARCELO FONSECA

ENGENHARIA SOCIAL: CONSCIENTIZANDO O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO

Esta Monografia foi julgada adequada à obtenção do título de Especialista em Inteligência de Segurança Pública e aprovado em sua forma final pelo Curso de Pós-Graduação *Lato Sensu* em Inteligência de Segurança Pública, da Universidade do Sul de Santa Catarina.

Brasília, 05 de maio de 2017.

Professor orientador: Camel André de Godoy Farah, Dr.

Universidade do Sul de Santa Catarina

Prof. Giovani de Paula, Dr.

Universidade do Sul de Santa Catarina

”É meu dever saber das coisas. Talvez eu tenha treinado para ver aquilo que os outros olham superficialmente.”

Sir Arthur Conan Doyle

AGRADECIMENTOS

Agradeço à Deus, por ter me agraciado com saúde e disposição que me permitiu realizar este trabalho.

À minha esposa e filho, pela compreensão e paciência durante minhas ausências para a realização deste trabalho.

Ao Professor e Orientador Camel André de Godoy Farah, por ter me ensinado e orientado de maneira inigualável sobre assuntos e temas relevantes para este trabalho.

Aos demais amigos e àqueles que, de alguma forma, contribuíram para a realização deste estudo.

RESUMO

Novas tecnologias surgem a cada dia objetivando preservar o sigilo das atividades de processamento, armazenamento, transmissão de dados digitais e comunicações, bem como integridade dos sistemas, materiais e programas de Tecnologia da Informação, no sentido de salvaguardar dados e conhecimentos.

Diante de tantos avanços tecnológicos e, consequentemente, a segurança da informação, o engenheiro social tem utilizado a psicologia para atacar o elo mais fraco de um sistema, o homem.

As deficiências naturais do ser humano podem ser exploradas muito mais facilmente que as de um software e os engenheiros sociais, sabendo dessa deficiência, explora as vulnerabilidades humanas para extrair a informação necessária.

Este trabalho visa alertar que gastos exorbitantes com tecnologias, por si só, não garantem inviolabilidade ou acesso ao dado sensível.

Palavras-chave: Engenharia Social, Elo mais fraco, Informação, Segurança da Informação

SUMÁRIO

1 INTRODUÇÃO..... 09

2 ELEMENTOS DA ENGENHARIA SOCIAL..... 11

2.1 O QUE É ENGENHARIA SOCIAL..... 11

2.2 TÉCNICAS EMPREGADAS PELO ENGENHEIRO SOCIAL..... 12

3 COMO EVITAR UM ATAQUE DE ENGENHARIA SOCIAL AO ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO 15

4 CONCLUSÃO..... 18

REFERÊNCIAS..... 19

1 INTRODUÇÃO

A cada dia a tecnologia se moderniza e paralelamente a essa modernização, ataques e defesas são frequentes no meio tecnológico. As empresas de Segurança da Informação se modernizam e dificultam os ataques cibernéticos.

Devido a essas dificuldades, os Engenheiros Sociais passaram a atacar diretamente os usuários desses sistemas, o homem. Apesar de todo investimento tecnológico das empresas, investe-se muito pouco em doutrinas de conscientização, naqueles que são considerados “O Elo mais Fraco”.

Os Engenheiros Sociais têm atacado cada vez mais as pessoas para atingirem seus objetivos. Eles exploram as “fraquezas” do homem, tais como, por exemplo: vaidade, autoconfiança e os sentimentos altruístas como necessidade de ser útil ou ajudar ao próximo, entre outros. A falta de conhecimento, o pensamento de que “isso nunca ocorrerá comigo”, facilita a investida de um Engenheiro Social, que pode utilizar diversas técnicas para atingir uma determinada “fraqueza” do alvo.

Diferentemente do que se pensa, o Engenheiro Social utiliza técnicas tolas e que aparentam ser bastante inofensivas. Por mais simples que pareça a técnica, se for utilizada de forma correta e com a pessoa certa, o dano pode ser devastador.

Ataques ao elo mais fraco são bem-sucedidos e, na maioria das vezes, com custo relativamente baixo, em função da ingenuidade do ser humano e da habilidade do Engenheiro Social. Muitas empresas ou pessoas não percebem que sofreram um ataque hostil, pois são usadas técnicas que dificultam a rastreabilidade das ações adotadas pelos engenheiros.

Os engenheiros sociais verificaram que é mais fácil obter dados de um ser humano do que de um computador, simplesmente porque as pessoas, muitas das vezes, não detém o conhecimento necessário para se proteger.

O ataque de um engenheiro social pode variar de ações simples até as mais elaboradas, como fazer parte do círculo social do alvo, ganhando confiança e meses depois, pedir alguma informação, objetivando adquirir a informação necessária.

Este tipo de ação tem êxito porque os humanos são susceptíveis a manipulação e podem ser persuadidos a fazer coisas, simplesmente por achar que está ajudando a uma pessoa.

Engenharia Social é uma prática utilizada para conseguir informações de interesse, utilizando habilidades como a persuasão, enganação, confiança das pessoas entre outras técnicas.

Novas tecnologias surgem a cada dia. Por conta desses avanços, empresas de segurança estão criando métodos para a proteção dos sistemas, minimizando as vulnerabilidades aos ataques e invasões.

Evitando as barreiras tecnológicas cada vez mais avançadas, os engenheiros sociais buscam obter acesso a informações sensíveis por meios dos que operam os sistemas, o ser humano. Por possuir vulnerabilidades comportamentais, psicológicas e desconhecimento da engenharia social, o ser humano é o meio mais comum de se obter dados negados.

O comportamento humano é complexo e por este motivo, cada um reage de uma maneira diferente à abordagem de um agressor. No entanto, podemos moldar algumas peculiaridades, fazendo com que o ser humano tenha ideia de que esteja sofrendo um ataque.

Diante das considerações acima, a relevância em escrever sobre Engenharia Social está em apresentar ao público alvo, o ser humano, as técnicas utilizadas pelos engenheiros sociais na obtenção de um dado sensível, mitigando a perda destes criando uma mentalidade de segurança no elo mais fraco.

Neste trabalho, a pesquisa sobre Engenharia Social é aplicada pois visa analisar métodos que dificultem a investida do Engenheiro Social. Pode ser usado em lares, pequenos empreendimentos ou em grandes empresas.

Visto que é preciso conhecer e analisar o conceito e as técnicas utilizadas pela Engenharia Social para dar início a um processo de educação continuada às pessoas, a pesquisa a ser realizada foi bibliográfica.

Fatores que envolvem os ataques do Engenheiro Social são apresentados e analisados, explicando as razões do sucesso do Engenheiro e maneiras de mitigar esses ataques.

2. ELEMENTOS DA ENGENHARIA SOCIAL

Esta pesquisa foi desenvolvida baseando-se na vulnerabilidade humana diante a um ataque de um Engenheiro Social.

2.1 O Que é Engenharia Social

Apesar de se tratar de uma técnica antiga, Mitnick foi um responsáveis pela popularização dessa arte nos anos 90, quando, aos 12 anos, usou a Engenharia Social para adquirir informações sobre os furos que os bilhetes de ônibus para fazer baldeações. Diante das informações obtidas, de um motorista a quem ficara amigo, do funcionamento daqueles furos, Mitinick passou a viajar para onde quisesse utilizando apenas um furador e bilhetes sem utilidade.

Analisando as palavras separadamente, de acordo com o dicionário PRIBERAM, tem-se:

1) Engenharia: conjunto de técnicas e métodos para aplicar o conhecimento técnico e científico na planificação, criação e manutenção de estruturas, máquinas e sistemas para benefício do ser humano.

2) Social: que diz respeito à sociedade.

De acordo com a Wikipédia, " refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais".

Para o hacker mais famoso do mundo Mitnick (2003), engenharia social é "habilidade de se manipular pessoas para obter informações necessárias para conseguir acessar um sistema, roubar dados de bancos ou qualquer outra coisa".

De acordo com estudos realizados em livros, monografias, artigos, entre outros, a melhor definição dada ao termo "Engenharia Social" é a seguinte: "Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para confirmar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos. (KONSULTEX, 2004 APUD PEIXOTO, 2006, p.4).

Diante da definição acima podemos destacar que o foco da Engenharia Social utiliza o desconhecimento do assunto e as vulnerabilidades humanas para lograr êxito em seus ataques.

2.2 Técnicas Empregadas pelo Engenheiro Social

A Engenharia Social tornou-se um dos maiores riscos de segurança de empresas e pessoas. As técnicas utilizadas pelos engenheiros estão cada vez mais sofisticadas e muitas das vezes, aproveitam-se das vulnerabilidades humanas, que na sua maioria não se dão conta de que estão sofrendo um ataque.

Inúmeras técnicas podem ser utilizadas pelo Engenheiro Social. A escolha da técnica estará condicionada ao grau de dificuldade e ao tipo de vulnerabilidade do alvo. Neste trabalho será citado alguns mais comuns:

2.2.1 Análise do Lixo

O lixo descartado por pessoas físicas ou jurídicas é uma das fontes mais ricas de informações para os engenheiros sociais. Por desconhecimento ou por acreditarem que "nunca acontecerá comigo", lixos são descartados diariamente sem nenhum tipo de tratamento de eliminação.

Engenheiros sociais realizam uma análise dos objetos que foram descartados pelo alvo, adquirindo informações e até rotinas, que podem ser utilizados pelos engenheiros.

Nos lixos descartados podem ser encontrados todo tipo de material útil, tais quais:

- Papéis classificados
- Nomes de usuários e senhas
- Papéis timbrados vazios
- Memorandos internos
- Rascunhos e minutas de documentos

2.2.2 Phishing

Os engenheiros sociais enviam e-mails, normalmente se passando por bancos, órgãos públicos ou uma notícia que esteja na moda e que atraia a atenção do alvo, objetivando obter

informações privilegiadas como nomes de usuários, senhas, dados sobre o cartão de crédito, entre outros.

A técnica do phishing geralmente está associado com a capacidade do engenheiro duplicar uma página web, para que o visitante acredite ser um site original. Para que este procedimento tenha sucesso, basta que o alvo clique em um link recebido pelo email, levando-o a um falso site.

2.2.3 Redes Sociais

Nos dias atuais, é cada vez mais comum a utilização das redes sociais para diversos tipos de atividades, tais como compartilhar informações, divulgar fotos ou vídeos, busca por emprego, entre outros. A possibilidade de inserção de dados a partir de smartphones tem facilitado a publicação e inserção de dados nessas redes sociais.

Há alguns anos, os usuário utilizavam com pouca frenquencia as redes sociais, hoje, porém, as redes sociais são utilizadas por muito mais pessoas, pela facilidade de comunicação com familiares e amigos.

Com a possibilidade de os usuários postarem vídeos, fotos, comentários, os usuários não limitam a quantidade de informações que postam diariamente nas redes sociais. Essas informações, por mais tola que pareça ao usuário, pode ser uma mina de ouro para o engenheiro social.

2.2.4 Internet Relay Chat (IRC)

O IRC é um protocolo de comunicação pela internet utilizado, basicamente, como chat ou bate-papo. É um grande meio de comunicação hoje em dia, permite que pessoas conversem com outras em tempo real. Geralmente o Engenheiro Social utiliza este meio para enganar uma pessoa, roubando-lhe uma informação de interesse.

Por este meio, um Engenheiro manipula suas vítimas com mentiras durante uma conversa, incentivando-as a clicar em uma foto ou link, ejecutando algum tipo de software malicioso.

São nos chats que pessoas ou grupo de pessoas conversam de forma anônima, favorecendo a abordagem íntima, visto que os Engenheiros sempre se utilizam das mentiras e falam coisas que agradam suas vítimas.

2.2.5 Telefone

O telefone é um dos meios mais utilizados pelos Engenheiros Sociais. O uso dessa técnica oferece vantagens tais como: a ocultação do número permite, em um primeiro momento, manter o anonimato de uma maneira simples; permite atuar a distância, o que dificulta a captura de um Engenheiro Social.

O Engenheiro costuma utilizar chamadas em cadeia, quando o objetivo é conseguir informações mais profundas de uma companhia. Faz-se uma primeira chamada, onde serão fornecidas informações sobre nomes de pessoas ou dados técnicos. Para conseguir essas informações, basta se passar por cliente ou possível patrocinador da empresa atacada. Na segunda chamada o atacante utiliza as informações obtidas na primeira chamada para que outra pessoa diferente da primeira chamada, passe informações ainda mais valiosas. Para que ninguém possa estabelecer uma conexão entre uma chamada e outra, as ligações não são realizadas consecutivamente. Há um intervalo considerável de tempo entre elas. É raro que um contato telefônico se mantenha por muito tempo. As ligações ocorrem até que o Engenheiro Social atinja seu objetivo.

2.2.6 Trojan Horse (Cavalo de Tróia)

Os trojans são mais uma forma de obtenção de informação. Com a utilização de um Trojan um Engenheiro pode tomar o controle de um computador, copiar arquivos, fazer cópia remota do disco rígido sem ser descoberto.

Um trojan é um tipo de software que pode entrar em um computador disfarçado como um programa legítimo, uma vez alojado no computador da vítima, realizandos malefícios que vão desde simples destruição de informação, o envio dessas informações a terceiros até roubo de senhas dos usuários.

3 COMO EVITAR UM ATAQUE DE ENGENHARIA SOCIAL AO ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO

Como mencionado no capítulo anterior, novas tecnologias e soluções de segurança surgem a cada dia, entretanto toda essa tecnologia não tem grande serventia se as pessoas não possuem consciência do valor das informações que elas tratam. De nada adianta ter um Firewall, Internet com VPN, transmissão de mensagens criptografadas se um usuário ingenuo ou desinformado clica em um link enviado por e-mail ou trata de assuntos sensíveis durante um cafezinho na copa da empresa onde trabalha?

IAN MANN (2011) demonstra que o elemento humano é crucial para a maioria dos ataques bem-sucedidos, segundo ele: "Pode ser útil pensar sobre segurança humana como o elo perdido entre a segurança em TI e a segurança física".

As pessoas mais vulneráveis a este tipo de ataques são aquelas que tratam informações sigilosas ou que podem permitir o acesso a elas e estas pessoas, por desconhecimento ou por excesso de confiança, deixam de tomar cuidados que afetam a segurança das informações sensíveis ou sigilosas.

Conforme CASTRO E SILVA e col. (2013, p.17):

> A falta de consciência dos utilizadores em relação aos perigos, a falta de conhecimento das técnicas de engenharia e o excesso de autoconfiança de muitos utilizadores são os elementos que promovem o sucesso da engenharia social.

Os Engenheiros se aproveitam do despreparo das pessoas para conseguir informações importantes e causar enormes danos ou prejuízos. O atacante utiliza-se da persuasão, fazendo-as acreditarem em algo que não é verdade.

Segundo Kevin D. Mitnick (2006), normalmente o Engenheiro Social utiliza as mesmas técnicas persuasivas que são utilizadas em nosso dia-a-dia, segundo ele: "...o engenheiro social aplica essas técnicas de uma maneira manipuladora, enganosa, altamente antiética, frequentemente com efeito devastador".

Para atingir seu objetivo, o engenheiro social se aproxima do seu alvo, conquistando sua confiança e atacando suas vulnerabilidades. Esta afirmação é reforçada por IAN MANN (2011) que cita:

> Apesar de ser amplamente ignorado pela indústria de segurança focada em TI, existe, na verdade, um longo histórico de hackers que exploram pessoas. O foco deles será o elo mais fraco em qualquer corrente de segurança.

Por este motivo, é essencial que entendamos alguns fatores humanos que são explorados pelo engenheiro, tais como:

- **Vaidade:** O ser humano, normalmente, possui um desejo de ser admirado por algo que tenha feito. O elo mais fraco costuma se vangloriar das coisas que faz, da imagem que passa para os outros. Conforme ADLER (1961, p. 189 APUD Souza Felipe):

  > a vaidade leva os indivíduos a pensar constantemente em si, ou quando não dê isso, na opinião dos outros a seu respeito.

- **Curiosidade:** A curiosidade é uma busca por novidades, representa um desejo humano de adquirir conhecimento e viver novas experiências. Todas as pessoas sentem curiosidades, mas o que se diferenciam são o alcance e a intensidade.

- **Persuasão:** Segundo definição do Wikipédia, persuasão "é uma estratégia de comunicação que consiste em utilizar recursos ou simbólicos para induzir alguém a aceitar uma ideia, uma atitude, ou realizar uma ação". Existe um poder para capturar o público, influenciar e motivar os indecisos. Não se trata de nenhum conhecimento mágico, mas proveniente da psicologia social. Segundo o Psicólogo Felipe, "Diversas pesquisas apontam que, com a complexidade da vida moderna, nós acabamos tomando a decisão de dizer sim e de comprar ou concordar com uma solicitação em questão de segundos ou minutos. Assim, ao contrário do que poderia parecer, persuadir (para o bem ou para o mal) não é algo difícil, complicado, extenuante".

- **Autoconfiança:** Este fator humano se refere em crer na própria capacidade para conseguir levar adiante uma determinada tarefa. É uma atitude que permite ao ser humano ter uma visão dele mesmo. As pessoas que possuem autoconfiança acreditam que possuem controle da própria vida e entendimento absoluto sobre um determinado assunto. O engenheiro social pode se aproveitar disso no momento em que a pessoa com autoconfiança passa determinados procedimentos ou informações sobre determinado assunto ou se prontificar a ajudar alguém com determinado assunto.

Para proteger informações, utiliza-se recursos tecnológicos de toda ordem, entretanto, basta uma pessoa ingênua, desinteressada por segurança ou desprevenida, para que todo aquele recurso tecnológico esteja vulnerável.

Visto que o engenheiro ataca, principalmente, o ser humano, educar e treinar as pessoas para o cumprimento de políticas de segurança, torna-se a principal defesa contra a Engenharia Social.

Como afirma Mitnick (2003): "como diz o ditado; até mesmo os verdadeiros paranoicos [sic] provavelmente têm inimigos. Devemos assumir que cada empresa também tem os seus – os atacantes que visam infra-estrutura [sic] da rede para comprometer os segredos da empresa. Não cabe sendo uma estatística nos crimes de computadores; está mais do que na hora de armazenar as defesas necessárias implementando controles adequados por meio de políticas de segurança e procedimentos bem planejados. (MITNICK; SIMON, 2003, p. 23)."

Política de Educação continuada pode ser definida como uma gama de informações dispostas de forma clara e concisa onde podem ser passadas diversas orientações àqueles que possuem ou podem ter acesso a informação. A política deve disciplinar e, acima de tudo, dever ser reforçada e fiscalizada a sua execução. Algumas orientações que podem estar contidas nessa Política de Educação continuada:

- Nunca revele por telefone ou e-mail dados sensíveis como senhas, informações pessoais, dados de cartão de crédito, entre outras.
- Nunca clique em links de site que cheguem através de e-mails ou por redes sociais e que não haja certeza da origem.
- Desconfie de qualquer mensagem de e-mail que ofereça facilidades e promoções fora do comum.
- Não fale mais do que o necessário com estranhos e tenha em conta que a Engenharia Social é uma técnica utilizada há centenas de anos. Muito antes da criação da internet, já se utilizava técnicas com objetivos maldosos.

4 CONCLUSÃO

A Engenharia Social é uma técnica muito utilizada por pessoas que desejam tomar posse de um dado negado a nível eletrônico ou pessoal, utilizando técnicas informáticas e pessoais, atacando principalmente as vulnerabilidades humanas, considerada o elo mais fraco no sistema de segurança. Este é um problema grave, já que a maioria das pessoas não possuem esclarecimentos suficientes sobre os riscos que estão correndo.

Não se trata somente de proteger nossos equipamentos tecnológicos com simples programas de antivírus e antispyware. As pessoas devem conhecer o modus operandi de um atacante, já que um simples convite de amizade no facebook pode comprometer toda a segurança de um sistema.

Um sistema de segurança não tem a ver somente com tecnologia, mas com processos. Diante disto, por mais avançado que seja a tecnologia, de nada adiantará se o fator humano não for considerado. É necessário conscientizar as pessoas de que ela pode estar sendo observada e que poderá se tornar um alvo em potencial de um Engenheiro Social.

Pessoas que detém algum conhecimento ou que podem servir de canal de acesso a um determinado dado, que seja de interesse de um engenheiro, deve receber treinamento de segurança da informação e medidas preventivas no trato de assuntos sigilosos, para que essas pessoas tenham habilidade em detectar, de maneira mais apurada, este tipo de ataque e saber como agir nesses casos.

A Engenharia Social é uma ameaça muito real e que, atualmente, tem domínio de ação, geralmente livre. Porém, isso não será sempre verdadeiro. Uma vez que se leve essa ameaça, verdadeiramente a sério e se aplique uma metodologia de prevenção, a Engenharia Social se tornará uma via muito mais difícil, se não impossível, de ser empregada por um engenheiro social.

REFERÊNCIAS

MITNICK, K. D.; SIMON, W. L. **A Arte de Invadir: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos**. São Paulo: Pearson, 2006.

ARAUJO, Eduardo E. de. **A Vulnerabilidade Humana na Segurança da Informação.** 2005. 85 f. Monografia (Graduação) – Faculdade de Ciências Aplicadas de Minas, União Educacional Minas Gerais S/C LTDA, Uberlândia, 2005. Acesso em: 20 de abril. 2017.

MANN, IAN. **Engenharia Social**. São Paulo: Blucher, 2011.

FONSECA, Paula F. **Gestão de Segurança da Informação**: O Fator Humano. 2009. 16 f. Monografia (Especialização)– Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: Acesso em: 15 mar. 2017.

GIAERDELLI, GIL. **Você é o que você compartilha: e-agora: como aproveitar as oportunidades de vida e trabalho na sociedade em rede**. São Paulo: Gente, 2012.

PRIBERAM. **Dicionário de Língua Portuguesa**. Disponível em:<www.priberam.pt/DLPO/> Acesso em 05 mar. 2017.

CASTRO E SILVA, FRANCISCO J. A. FARIA, **Classificação Taxonómica dos Ataques de Engenharia Social**. Disponível em: http://repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf. Acesso em: 20 janeiro 2017.