HUMANO: A FALHA MAIS GRAVE DE UM SISTEMA

DA SILVA. Pedro Davi Dantas [1] (FAFIC)
MACIEL, Saymon Bezerra de Sousa [2] (ORIENTADOR)

INTRODUÇÃO

Engenharia Social é o termo usado para definir um método de ataque, no qual é feito o uso da persuasão, abusando da confiança da vítima, para a obtenção de informações que possam ser utilizadas para um acesso não autorizado a computadores ou informações.

PROBLEMÁTICA

Como as empresas e as pessoas em geral estão em relação à Engenharia Social? Estão preparados para este tipo de ataque em suas vidas? Assim, a importância do tema deve-se ao fato de que muitas pessoas estão desprevenidas quando sofrem este tipo de ataque, principalmente no que se refere aos ataques que envolvem psicologicamente.

OBJETIVO

Demonstrar a quantidade de pessoas vulneráveis atualmente, mesmo com tanto acesso a informação, e também promover o conhecimento sobre o assunto, bem como práticas de prevenção e defesa, com o intuito de que o leitor possa refletir melhor antes de confiar nas pessoas para ceder informações.

METODOLOGIA

A pesquisa foi baseada no modelo descritivo, através do qual o assunto foi estudado minuciosamente, foram coletados dados qualitativos e quantitativos. Para constituir a pesquisa foi feito um estudo no qual aplicou-se a Engenharia Social. Percebemos que no atual contexto o desemprego seria um ponto relevante para elaborar e planejar um ataque rápido e eficaz.

Primeiro procedimento: Criação de pessoa fictícia, com dados completos.

Segundo procedimento: Criação de rede social.

Terceiro procedimento: Começar a interação com pessoas.

[1] Bacharelando em Ciência da Computação - Faculdade de Filosofia Ciências e Letras de Cajazeiras – FAFIC.
[2] Mestrando no Programa de Pós-graduação em Sistemas Agro-industriais (PPGSA). Graduado em Análise e Desenvolvimento de Sistemas pela Faculdade Leão Sampaio (FALS). Professor da Faculdade de Filosofia Ciências e Letras de Cajazeiras – FAFIC.

Quarto procedimento: Solicitamos acesso a grupos de venda da região e aproveitando-se da conjuntura socioeconômica, utilizamos uma oferta de emprego fácil.

Após a publicação, diversas pessoas mostraram interesse. Contatamos estas pessoas com uma mensagem bastante genérica. Com esta mensagem, formal e educada, conseguimos muitos e-mails.

Sexto procedimento: Criação de site fictício de empresa com informações e layout.

Sétimo procedimento: Criação de um pequeno arquivo de lote do Windows (.BAT), com apenas uma instrução de contagem e um redirecionamento para nosso site fictício. Arquivo que foi convertido para um executável (.EXE) que continha um ícone da empresa fictícia. Obs.: O arquivo não conteve nenhum código malicioso, mas apenas de contagem e inicialização do site fictício que também não continha código malicioso.

Oitavo procedimento: Criação de um formulário para coleta de dados dos interessados.

Nono procedimento: Entramos em contato com as pessoas interessadas mais uma vez com uma mensagem genérica e um e-mail em massa, contendo todos os e-mails já coletados até então. A mensagem genérica enviada a todas as pessoas pedia que seguissem instruções para baixar o arquivo, assim como preencher o formulário.

Notamos que de 28 pessoas, 26 caíram no golpe e fizeram todas as instruções que pedimos. Pois ao instalar nosso suposto arquivo de módulo de segurança, foi contado o registro da pessoa que clicou no arquivo, o qual poderia ser um vírus. Já quanto ao formulário, dentre as 28 pessoas, 20 preencheram, assim podendo ser coletados dados importantes que permitiriam outros tipos de ataques, tanto de Engenharia Social como acesso forçado de contas e e-mails, pois segundo estudos a maioria das pessoas utiliza a mesma senha para tudo, o que também se aplica quando perguntamos no formulário qual senha desejariam como acesso ao nosso sistema, de forma que poderíamos aplicar já outro tipo de ataque. Tais resultados já denotam uma preocupação maior.

FUNDAMENTAÇÃO TEÓRICA

Mitnick (2001-2005) nos seus livros, relata a forma de pensar para planejar ataques. Ian Mann (2011) relata as várias formas de prevenção e combate contra estes tipos de ataques.

CONSIDERAÇÕES FINAIS

Alguns exemplos de ataques: executar um programa, acessar uma página falsa de comércio eletrônico ou de banco através de um link em e-mail, página e WhatsApp.

Para se prevenir o bom senso é crucial, desconfiar de qualquer abordagem, via rede social, e-mail ou telefone, na qual uma pessoa solicita informações suas principalmente confidenciais. Nunca forneça muitas informações, e nunca forneça informações como senhas ou números de cartões de crédito. Em caso de recebimento de mensagens deste tipo, procurando a lhe induzir a baixar e executar programas, clicar em um link enviado por e-mail ou acessar uma página web, é se suma importância que antes que você faça qualquer ação, procure identificar e entrar em contato com a instituição envolvida. No caso de pessoa comum onde não há envolvimento de empresas, investigue, faça perguntas e desconfie.

REFERÊNCIAS

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar**: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. 1ª. ed. [S.l.]: Person Education, 2001. 304 p.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Invadir**: As verdadeiras histórias por trás de ações de hackers, intrusos e criminosos eletrônicos. 1ª. ed. [S.l.]: Prentice Hall, 2005. 236 p.

MANN, Ian. **Engenharia Socia**l: Série de Prevenção e Fraudes. 1ª. ed. São Paulo: Blucher, 2011. 236 p.

Palavras-chaves: Engenharia Social, Segurança da Informação, Falha Humana.