Markus Vinicyus P. Guimarães e Lucas Aparecido De Jesus

Engenharia Social em Nosso Cotidiano

19 de Agosto de 2017

Markus Vinicyus P. Guimarães e Lucas Aparecido De Jesus

Engenharia Social em Nosso Cotidiano

19 de Agosto de 2017

Sumário

1 Introdução

Atualmente, o uso da tecnologia vem crescendo no mundo todo, e com isso a complexidade para invadir um sistema também(computador a computador) e por isso se faz o uso da engenharia social.

Engenharia social é o termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão e muita das vezes se passando por uma pessoa com influência e autoridade, abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores e/ou outras informações.

Este trabalho pretende mostrar e compreender como os sistemas são falhos não somente porque os seus computadores estão desatualizados ou por qualquer vulnerabilidade em sua rede, mas sim porque todo sistema em algum momento envolve pessoas. O fator humano é algo que não se pode calcular, que não se pode prever, ou seja, só se pode corrigir, ou pelo menos tentar se corrigir, após o acontecimento da invasão, o que torna a engenharia social uma ótima técnica.

2 Justificativa

Este trabalho justifica-se pelo fato de que a tecnologia faz cada vez mais parte da vida das pessoas e ao em vez de treinar seu pessoal, empresas se preocupam notavelmente mais com as máquinas. Fora o usuario comum, que sem muito conhecimento, ficam a mercê desses criminosos.

Nos últimos tempos os sistemas vem sim ficando mais seguros, com diversos avanços tecnológicos, os softwares estão cada vez mais difíceis de se penetrar, porém há uma falha que pode ser considerada mais perigosa no processo, as pessoas.

Por diversos motivos as pessoas são uma vunerabilidade no sistema, a pressa faz que muita das etapas de verificação de segurança, que deveriam se feitas sejam puladas, pois muitos consideram essas etapas apenas burócracia. O medo de ser demitido, faz com que identidades de supostos superiores não sejam conferidas, e o principal, a falta de fé das pessoas que um golpe pode acontecer com elas.

3 Objetivos

3.1 Objetivo Geral

Mostrar a necessidade em se proteger das ameaças em sua empresa, ou até mesmo, em sua casa e apresentar as principais praticas de engenharia social.

3.2 Objetivos Específicos

- Por meio de uma pesquisa descobrir os principais problemas sofridos por usuários e empresas em relação a vazamentos por funcionarios, dentre eles, os principais golpes sofridos, os principais descuidos com questão à segurança de seus dados, etc.
- Por meio de um levantamento entender como é o comportamento das pessoas em relação a segurança.
- Por meio de uma pesquisa descobrir as principais ferramentas e práticas para se proteger dos invasores que usam dessa prática, assim como, formas de pessoas comuns se protegerem em seu cotidiano.

4 Metodologia

Será realizada uma vasta pesquisa bibliográfica a partir de artigos científicos, livros, dissertações e teses, para entender como se proteger no meio virtual.

Também será realizada uma pesquisa de Levantamento, na qual será questionada diretamente as pessoas usando a ferramenta google formulários, para conhecer o comportamento destas pessoas em relação a confiança que tais tem nos outros e como isso afeta suas vidas.

Também terá um levantamento sobre os ataques feitos através das redes sociais são praticamente diários. E Com esse levantamento notar a falha das pessoas diate de um ataque da engenharia social. Segundo Pedro Cipoli com o tempo os ataques feitos pode-se identificar com relativa facilidade aquele e-mail que solicita nossa "alteração cadastral"ou dizendo que precisamos "mudar nossa senha bancária conforme a política de segurança". Alguns desses ataques nosso bom e velho antivirus consegue até nos alertar.

Mas não existe essa possibilidade quando se trata de relacionamentos interpessoais não envolvendo computadores, o que nos deixa claramente muito vulneráveis.(CIPOLI, 2017)

5 Desenvolvimento

A Engenharia Social é uma técnica antiga e muito popular, que poderia ser traduzida, grosso modo, como "enganar pessoas". A ideia é que o engenheiro social, como são conhecidos aqueles que praticam essa ato, possa manipular pessoas para que elas revelem informações importantes ou, então, para que elas façam algo que facilite o trabalho dele.Além disso, ela também pode ser encarada como uma maneira de tirar proveito em benefício próprio, por meio de truques psicológicos, ao manipular a tendência que as pessoas possuem de confiar umas nas outras. Autoconfiança, facilidade de comunicação, aptidão profissional e grande capacidade de persuasão são características de um engenheiro social. Muitas vítimas de ataques afirmam que mal sabem que passaram informações que não deveriam devido ao talento da pessoa com quem conversou, e esse caso não é tão improvável quanto pensamos.

5.1 Fator Humano na Engenharia Social

Segundo Albert Einstein somente duas coisas são infinitas: o Universo e a estupidez humana. E não estou seguro quanto à primeira(EINSTEIN, 1996). Com isso a engenharia social vem tirando proveito das pessoas ingênuas pois são elas que darão as informações precisas para que o invasor obtenha o que deseja. O invasor aproveita da pressa, e até mesmo do medo de funcionários para obter acesso indevido a informações.Também o processo de Engenharia Social em alguns casos são totalmente praticados fora do ciberespaço, onde a capitação de informações é feita através de táticas bem trabalhadas de relacionamento interpessoal. A prática de iludir e induzir pessoas para involuntariamente ceder informações restritas remonta de muito tempo e com o avanço da tecnologia e dos ciberespaços, abre-se um novo campo para os ataques dos engenheiros sociais. Sendo o contato pessoal o primeiro passo na artimanha da engenharia social, devemos nos atentar as táticas utilizadas e as técnicas de proteção que devemos aplicar para não nos tornarmos um canal de fornecimento de informações restritas.

Por exemplo, o invasor ciente que o dono de uma empresa visitara uma determinada filial, o invasor se antecipa e se passa por ele antes de sua chegada, o invasor pede alguns dados, e o funcionário por medo de colocar seu emprego em risco passa essas informações sem pedir uma comfirmação de indentidade, a final, não existe a possibilidade de não ser ele, não é mesmo?(SIMON, 2001)

5.2 Formas de Persuasão

Os próprios hackers vêem a engenharia social de um ponto de vista psicológico, enfatizando como criar o ambiente psicológico perfeito para um ataque. Os métodos básicos de persuasão são: personificação, insinuação, conformidade, difusão de responsabilidade e a velha amizade. Independente do método usado, o objetivo principal é convencer a pessoa que dará a informação, de que o engenheiro social é, de fato uma pessoa a quem ela pode confiar as informações prestadas. Outro fator importante é nunca pedir muita informação de uma só vez e sim perguntar aos poucos e para pessoas diferentes, a fim de manter a aparência de uma relação confortável. Personificação geralmente significa criar algum tipo de personagem e representar um papel. Quanto mais simples esse papel, melhor. Às vezes, isto pode ser apenas ligar para alguém e dizer: "Oi, eu sou Marcos do setor de informática e preciso da sua senha". Mas isto nem sempre funciona. Outras vezes, o hacker vai estudar uma pessoa de um departamento e esperar até que se ausente para personificá-la ao telefone. De acordo com Bernz (1996), um hacker que escreveu extensivamente sobre o assunto, eles usam pequenas caixas para disfarçar suas vozes e estudam os padrões de fala. Este tipo de ataque é menos freqüente, pois exige mais tempo de preparo, mas acontece. Outra tática comum que pode ser utilizada num ataque de personificação é o hacker se passar por assistente da gerência ou mesmo presidência e pedir a um funcionário, em nome do seu superior, alguma informação. Para não criar atritos com seu superior, o usuário fornece as informações sem muitos questionamentos. Numa grande empresa, não há como conhecer todos os funcionários; então, fingir uma identidade não é um truque muito difícil de ser aplicado.

5.3 Como Funciona os ataques de Engenharia Social

Eles usam técnicas do tipo com o objetivo de ganhar acesso legítimo à rede e aos dados da empresa roubando credenciais de usuários autorizados para se passar por funcionários da própria empresa.Esse tipo de cibercriminoso se aproveite da inocência e da natureza prestativa de alguns usuários. Eles podem, por exemplo, ligar para algum deles simulando ter de resolver algum incidente, dizendo então que necessita do acesso urgente à rede corporativa.Os ataques também podem ser feitos por meio das redes sociais.Os cibercriminosos podem apelar a uma série de sentimentos por meio dos perfis de redes sociais das vítimas, descobrindo, por exemplo, sua posição dentro da empresa, seus amigos e seus gostos pessoais.A engenharia social não é exclusivamente utilizada em informática, a engenharia social é uma ferramenta onde exploram-se falhas humanas em organizações físicas ou jurídicas onde operadores do sistema de segurança da informação possuem poder de decisão parcial ou total ao sistema de segurança da informação seja ele físico ou virtual, porém devemos considerar que as informações pessoais, não documentadas, conhecimen-

tos, saber, não são informações físicas ou virtuais, elas fazem parte de um sistema em que possuem características comportamentais e psicológicas na qual a engenharia social passa a ser auxiliada por outras técnicas como: leitura fria, linguagem corporal, leitura quente, termos usados no auxílio da engenharia social para obter informações que não são físicas ou virtuais mas sim comportamentais e psicológicas

5.4 Truques mais comuns na Engenharia social

5.4.1 1° Tática (Empresas)

A maior parte das empresas reaproveita folhas de sulfite para impressões de documentos que circularão apenas internamente. Essa é uma prática que traz economia e, ao mesmo tempo, demonstra uma preocupação ambiental. Porém, não é raro encontrar na pilha de papéis reaproveitáveis alguns demonstrativos ou relatórios internos que possam ter informações secretas. Ainda pior, pode ser que você encontre até folhas com a palavra "CONFIDENCIAL" estampada no cabeçalho, o que deixa muito mais vuneravel essas informações secretas uma vez que o invasor consegue acesso interno a impresa, pois não depende nem mesmo dos funcionários.(TECHMUNDO, 2011)

5.4.2 2° Tática (Setores Desprotegidos)

Uma prática comum para entrar em setores protegidos é aproveitar a entrada de alguém. Quando o invasor observa que a porta para o local foi destravada por outro, ele chega de surpresa, sorridente, dizendo que vai aproveitar a "carona". Isso provavelmente não funcionaria em uma empresa com poucos funcionários, mas em grandes corporações, que ocupam diversos andares, é muito provável que confundam o invasor com um funcionário novo ou ainda desconhecido. Um Engenheiro Social também pode entrar alegando que esqueceu o cartão de funcionário em casa, um invasor pode acabar descobrindo falhas no sistema de catracas da entrada do edifício comercial. Muitos desses sistemas não funcionam bem ou são simplesmente ignorados por quem devia ler os relatórios de entrada e saída dos funcionários.(TECHMUNDO, 2011)

5.4.3 3° Tática (Internet)

Um truque também muito comum é o invasor se passar por administrador da rede ou técnico de um serviço que possa estar apresentando "problemas". Com essa abordagem, pode ser que ele consiga o usuário e a senha da vítima. E já que muitas pessoas costumam usar a mesma senha para diversos perfis online, o agressor acaba tendo acesso a uma grande quantidade de informações pessoais da vítima.(TECHMUNDO, 2011)

5.4.4 Phishing

O phishing ocorre quando um hacker produz comunicações fraudulentas que podem ser interpretadas como legítimas pela vítima por alegarem vir de fontes confiáveis.

Em um ataque de phishing, os usuários podem ser coagidos a instalar um malware em seus dispositivos ou a compartilhar informações pessoais, financeiras ou de negócio.

Apesar de o e-mail ser o modo mais tradicional para o envio de phishing, esse tipo de ataque também pode vir na forma de um contato telefônica ou de uma mensagem no Facebook, por exemplo.

Os piores ataques de phishing se aproveitam de situações trágicas com o objetivo de explorar a boa vontade das pessoas, fazendo com que passem informações pessoais e de pagamento para realizar doações.

5.4.5 Baiting

A intenção é despertar a curiosidade do indivíduo para que insira o dispositivo em uma máquina a fim de checar seu conteúdo.

O sucesso dos ataques de baiting depende de três ações do indivíduo: encontrar o dispositivo, abrir seu conteúdo e instalar o malware sem perceber. Uma vez instalado, o malware permite que o hacker tenha acesso aos sistemas da vítima.

A tática envolve pouco trabalho por parte do hacker. Tudo que ele precisa fazer é infectar um dispositivo e ocasionalmente deixá-lo à vista do alvo, seja na entrada ou no interior dos escritórios. O dispositivo pode ser, por exemplo, um pen-drive contendo um arquivo com nome “chamativo”.

5.4.6 Técnica usada por Kevin Mitcnick

O famoso hacker Kevin Mitcnick foi um dos responsáveis pela popularização do termo Engenharia Social. Em seu livro “A arte de enganar”, Mitnick conta que teve o primeiro contato com a técnica aos 12 anos, quando percebeu que os bilhetes usados para as baldeações de ônibus usavam um esquema peculiar de furos em papel, utilizados pelos motoristas para marcar o dia, a hora e o itinerário das viagens.Uma das diversões do jovem phreaker era conversar com atendentes que pudessem alterar a classe de serviço dos amigos. Assim, quando um deles pegava o telefone de casa para fazer uma ligação, uma mensagem eletrônica pedia para que eles depositassem 25 centavos para poder concluí-la, como se eles estivessem discando a partir de um telefone público.(MITNICK, 2011)

5.4.7 Técnica ultilizada por Abraham Abdallah

Abraham Abdallah usado revista Forbes para encontrar celebridades alto patrimônio líquido , em seguida, enviou cartas para agências de referência de crédito em papel tim-

brado da empresa falsos pedindo mais informações. Ele então usou endereços, números de segurança social e outras informações de identificação a partir dessas correspondências para abrir cartões de crédito , ter acesso a contas bancárias e geralmente roubar identidades das pessoas mais ricas. Este é um exemplo de engenharia social por causa de seus papéis timbrados da empresa - ele ganhou a confiança através de um disfarce, que ele então usado para roubar dinheiro.

5.5 Redes Sociais

Os chamados imitadores de redes sociais estão cada vez mais atuantes no Facebook, Twitter, Instagram, Snapchat, YouTube e também no LinkedIn. O alvo desses "trapaceiros" são os perfis autênticos e, por meio de técnicas de engenharia social, eles tentam acessar dados sensíveis das empresas.Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem uso da tecnologia".E atualmente muitas informações podem ser coletadas através da internet e redes sociais, acessadas no mesmo smartphone que o usuário usa para suas tarefas corporativas. Quando um engenheiro social precisa conhecer melhor seu alvo, sai em busca nas redes sociais de informações interessantes de funcionários da empresa, cargos, amizades, perfil pessoal, entre outros. As redes sociais servem para conectar pessoas, e um perfil pessoal ou corporativo falso, mas convincente, ou uma solicitação para se conectar, pode ser o suficiente para aplicar um golpe de engenharia social.

5.6 Formas de Prevenção

A prevenção não é uma tarefa fácil. A maioria das empresas não direciona recursos financeiros nem humanos para tal. No entanto, investem na manutenção de sistemas e em novas tecnologias, ao invés de direcionar parte desse investimento para combater um inimigo que pode ser bem mais perigoso, a engenharia social. A ameaça deste inimigo é real, tanto quanto as falhas em uma rede. Os seres humanos são seres imperfeitos e multifacetados. Além disso, situações de risco modificam seus comportamentos, e, decisões serão fortemente baseadas em confiança e grau de criticidade da situação. Em função desses fatores, sempre existirão brechas em seu caráter ou comportamento pouco consciente com relação à segurança, onde a engenharia social poderá ser plenamente eficaz. Para amenizar estes riscos, é recomendável que as empresas criem políticas de segurança centralizada e bem divulgada, para que todos os seus colaboradores saibam como proteger as informações que estão em seu poder. As intranets11 podem ser um recurso valioso para esta divulgação, assim como boletins periódicos on-line, lembretes no correio eletrônico, requisitos de mudança de senha e treinamento. O maior risco é de os funcionários tornarem-se complacentes e relaxarem na segurança; por isso a importância da insistência.

O treinamento deve estender-se por toda a empresa. Diretores, gerentes, supervisores, e demais funcionários, todos devem ser treinados. Nestes treinamentos devem ser exploradas as táticas comuns de intromissão e as estratégias de prevenção. Quando alguém captar sinais de um ataque, deve imediatamente alertar os demais, para que não sejam também abordados.

6 Cronograma

Tabela 1 –

Meses	Agosto	Setembro	Outubro	Novembro	Dezembro
Levantamento Bibliográfico					
Implementação da Proposta					
Testes					
Analises dos Resultados					
Apresentação					

Referências

CIPOLI, P. *O que é Engenharia Social*. 2017. Disponível em: <https://canaltech.com.br/seguranca/O-que-e-Engenharia-Social/>.

EINSTEIN, A. *Albert Einstein Die Philosophin*. 1996. Disponível em: <https://www.pensador.com/frase/MjQ3Mw/>.

MITNICK, K. *Engenharia Social: o malware mais antigo do mundo*. https://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm: Felipe Arruda, 2011.

SIMON, K. M. . W. *A arte de Enganar*. https://www.docdroid.net/Mq0Edkm/kevin-mitnick-a-arte-de-enganar.pdfpage=15: John Wiley & Sons, 2001. Página 15.

TECHMUNDO. *Engenharia Social: o malware mais antigo do mundo*. 2011. Disponível em: <https://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm>.