VIII SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317-8302
8TH INTERNATIONAL CONFERENCE
CYRUS Institute of Knowledge MAKE A DIFFERENCE

Engenharia Social no Ambiente Corporativo

Social Engineering in the Corporate Environment

RENNAN RICHARD SANTOS SOUZA
UNINOVE – UNIVERSIDADE NOVE DE JULHO

CLAUDINEIA HELENA RECCO
UNINOVE – UNIVERSIDADE NOVE DE JULHO

MARCELO ELOY FERNANDES
UNINOVE – UNIVERSIDADE NOVE DE JULHO

Nota de esclarecimento:
Comunicamos que devido à pandemia do Coronavírus (COVID 19), o VIII SINGEP e a 8ª Conferência Internacional do CIK (CYRUS Institute of Knowledge) foram realizados de forma remota, nos dias **01, 02 e 03 de outubro de 2020.**

VIII SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317-8302
8TH INTERNATIONAL CONFERENCE
CYRUS Institute of Knowledge
MAKE A DIFFERENCE

Engenharia Social no Ambiente Corporativo

Objetivo do estudo
Os objetivos gerais desse artigo são: mostrar como as pessoas são enganadas pelo engenheiro social, quais técnicas são utilizadas, engenheiros sociais mais conhecidos, o objetivo do atacante e como mitigar os ataques para proteger as informações. Os objetivos específicos são: Mostrar o ciclo de ataque de engenharia social, conceito de dados e informação, valor da informação para as organizações e o valor da informação para os engenheiros sociais, como são realizados os ataques de Phishing, vishing, Smishing, dumpster diving, Shoulder Surfing, tailgate, abordagem pessoal, ataques por telefone, engenharia social reversa, os prejuízos financeiros, política de segurança para amenizar esses ataques, treinamento, conscientização dos colaboradores etc.

Relevância/originalidade
A escolha do tema "engenharia social" foi porque as empresas precisam constantemente proteger suas informações e certamente necessitam de pessoas para manter a confidencialidade. As organizações precisam estar atentas para a segurança de seus colaboradores, ou seja, necessitam tomar medidas para mitigar o ataque de engenharia social.

Metodologia/abordagem
Estudo bibliográfico com apoio nas obras extraídas de periódicos, anais de congressos e literatura relacionada ao tema.

Principais resultados
Em virtude dos fatos mencionados nesse artigo, pode-se ter uma noção da preciosidade da informação para as organizações, investimentos somente em equipamentos técnicos não surtem resultados positivos se o lado humano for ignorado. Por isso, o engenheiro social visa explorar os sentimentos das pessoas com a ajuda de técnicas específicas.

Contribuições teóricas/metodológicas
Ao realizar um estudo a cerca do tema engenharia social os autores corroboraram com a revisão bibliográfica de forma a expandir o conhecimento sobre o tema.

Contribuições sociais/para a gestão
Portanto, corporações que deixavam a informação confidencial somente com um colaborador estavam mais propensas de sofrer os ataques. Pode-se notar que a porcentagem de empresas que priorizam a segurança desse ativo é equilibrada, porém, quem não deixou bem clara a política de segurança da informação em conjunto aos treinamentos e conscientizações sobre os perigos da engenharia social teve perdas financeiras muito altas. Conclui-se que as pessoas são as mais frágeis no ambiente corporativo e que nenhuma organização está completamente segura mesmo se for aplicado medidas para amenizar esses incidentes, pois sempre haverá funcionários com informações importantes e engenheiros sociais com o interesse em obter esse ativo, ou seja, nada nesse mundo é 100% seguro.

Palavras-chave: Engenharia social, reversa, reversa, segurança da informação, corporativo

VIII SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317-8302
8TH INTERNATIONAL CONFERENCE
CYRUS Institute of Knowledge
MAKE A DIFFERENCE

Social Engineering in the Corporate Environment

Study purpose
The general objectives of this article are: to show how people are deceived by the social engineer, what techniques are used, best-known social engineers, the attacker's goal and how to mitigate attacks to protect information. The specific objectives are: To show the social engineering attack cycle, the concept of data and information, the value of information for organizations and the value of information for social engineers, how Phishing, vishing, Smishing, dumpster diving attacks are carried out , Shoulder Surfing, tailgate, personal approach, telephone attacks, reverse social engineering, financial losses, security policy to mitigate these attacks, training, employee awareness etc.

Relevance / originality
The choice of the "social engineering" theme was because companies constantly need to protect their information and certainly need people to maintain confidentiality. Organizations need to be aware of the safety of their employees, that is, they need to take measures to mitigate the attack of social engineering.

Methodology / approach
The choice of the "social engineering" theme was because companies constantly need to protect their information and certainly need people to maintain confidentiality. Organizations need to be aware of the safety of their employees, that is, they need to take measures to mitigate the attack of social engineering.

Main results
Due to the facts mentioned in this article, one can have a sense of the preciousness of information for organizations, investments only in technical equipment do not yield positive results if the human side is ignored. Therefore, the social engineer aims to explore people's feelings with the help of specific techniques.

Theoretical / methodological contributions
When carrying out a study on the topic of social engineering, the authors corroborated the bibliographic review in order to expand knowledge on the topic.

Social / management contributions
Therefore, corporations that left confidential information with only one employee were more likely to suffer the attacks. It can be noted that the percentage of companies that prioritize the security of this asset is balanced, however, those who did not make the information security policy in conjunction with training and awareness about the dangers of social engineering very clear had very high financial losses.

Keywords: Social engineering, Reverse, Attacks, ENVIRONMENT, information security

1 Introdução

A partir do surgimento da globalização, a informação se transformou em um recurso essencial para as organizações gerarem mais inovações para sobreviverem no mercado. As pessoas são elementos fundamentais para as organizações, tem o papel de guardar informações e gerar resultados positivos para melhorar a competitividade.

O incidente ocorrido no dia 11 de setembro de 2001 fez com que todas as organizações pensassem em novas formas de proteger a informação. Com a evolução da tecnologia, surgiram novas brechas na segurança da informação, muitas empresas passaram a se preocupar mais com a segurança de suas informações, começaram a investir pesado em sistemas e equipamentos para manter a proteção.

Entretanto, mesmo as organizações gastando bastante dinheiro para se proteger o máximo possível, existem vulnerabilidades nas pessoas que podem ser exploradas pelo engenheiro social e este deseja obter as informações confidenciais das empresas através dos colaboradores a qualquer custo. Muitos colaboradores estão sofrendo ataques de engenharia social. As pessoas são as principais responsáveis das informações em uma organização, são muito frágeis, tem comportamentos e sentimentos e os mesmos podem ser afetados.

Os objetivos gerais desse artigo são: mostrar como as pessoas são enganadas pelo engenheiro social, quais técnicas são utilizadas, engenheiros sociais mais conhecidos, o objetivo do atacante e como mitigar os ataques para proteger as informações.

Os objetivos específicos são: Mostrar o ciclo de ataque de engenharia social, conceito de dados e informação, valor da informação para as organizações e o valor da informação para os engenheiros sociais, como são realizados os ataques de *Phishing, vishing, Smishing, dumpster diving, Shoulder Surfing, tailgate,* abordagem pessoal, ataques por telefone, engenharia social reversa, os prejuízos financeiros, política de segurança para amenizar esses ataques, treinamento, conscientização dos colaboradores etc.

A escolha do tema “engenharia social” foi porque as empresas precisam constantemente proteger suas informações e certamente necessitam de pessoas para manter a confidencialidade. As organizações precisam estar atentas para a segurança de seus colaboradores, ou seja, necessitam tomar medidas para mitigar o ataque de engenharia social.

Nesse contexto, apresentar ataques de engenheiros sociais, técnicas e meios de defesas para minimizar o roubo de informações. Esse trabalho de conclusão de curso terá como foco a engenharia social no ambiente corporativo.

As organizações são alvos dos engenheiros sociais, porque suas políticas de segurança da informação não são adequadas, por falta de treinamentos para todos os colaboradores e falta uma conscientização a respeito dos perigos, isso favorece o atacante a explorar a vulnerabilidade conhecida por muitos, ou seja, as pessoas que por terem sentimentos estão sujeitas a confiar em qualquer outra, e esta pessoa pode ser um engenheiro social.

As organizações têm suas informações confidenciais descobertas, porque o engenheiro social utiliza procedimentos diferentes em determinadas pessoas para roubar esse ativo das empresas.

O engenheiro social necessita dessas informações confidenciais, porque o objetivo dele é vender para empresas concorrentes, pegar o dinheiro facilmente das vítimas ou até mesmo fazer uma vingança.

Para o desenvolvimento desse artigo haverá pesquisas bibliográficas nos seguintes livros: A arte de enganar – autor: Kevin Mitnick e Willian L. Simon, Engenharia social – autor: Iann Mann e algumas pesquisas em materiais disponíveis na internet. O objetivo é mostrar o que é engenharia social e que todos os funcionários podem ser vítimas do engenheiro social e também como adicionar medidas para mitigar os ataques.

1. ENGENHARIA SOCIAL

A engenharia social é usada para explorar a parte mais fraca de uma organização. O aspecto principal é fazer com que as vítimas executem ações solicitadas pelo atacante (DIOGENES, 2011).

A obtenção dessas informações é feita diante da pessoa ou através de um computador ou outro dispositivo, análise de lixo das organizações ou pelo monitoramento da rotina de possíveis vítimas, portanto, o engenheiro social faz ataques diretos e indiretos.

De acordo com Mitnick e Simon:

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia (2003, p.8).

Geralmente não está ligada sempre ao uso da tecnologia, ou seja, por meio de uma mera conversa com o alvo é possível obter informações sem levantar suspeitas (DIOGENES, 2011).

Engenharia social é o ato de uma pessoa utilizar técnicas para fazer com que outras pessoas passem informações, ou seja, qualquer tipo de informação que o engenheiro social possa conseguir de uma determinada empresa terá um significado, portanto, a coleta é realizada para poder traçar seu plano de ação em suas vítimas que serão escolhidas.

Sendo assim, "a engenharia social pode ser usada para obter diretamente informações confidenciais, apesar de muitas vezes as informações não terem sido classificadas de nenhuma maneira" (Mann, 2011, p.19).

2.1. O valor da informação para as organizações e para o engenheiro social

A informação é um ativo fundamental para as empresas, só é válida se estiver em confidencialidade, ou seja, se for pública não terá valor para a tomada de decisão.

"A informação é um bem que tem alto valor para a empresa, mas este bem só poderá ser utilizado se for devidamente protegido. A informação protegida proporciona a organização tomar decisões precisas para os seus negócios" (Nascimento, 2013, p.1).

Proporciona benefícios para as organizações manterem a competitividade, como exemplo a inovação ou a melhoria de um produto. Além de representar sua notoriedade no mercado a informação também adiciona mais credibilidade para quem a possuir.

"A informação traz vantagens competitivas em qualquer cenário: financeiro, comercial, industrial, político e militar. Portanto, informação tem valor agregado" (Svaiter, 2015, p.1).

A informação tornou-se muito relevante para as organizações usufruírem dessa preciosidade, por isso, deve haver um grau de classificação da informação para saber qual deve ser protegida.

De acordo com Orlandini:

> A informação é obtida através da organização de diversos dados, atribuindo-lhes valores e significado. Criar sistemas de gestão dessa "ordenação de dados" é uma tarefa complexa e que exige grande comprometimento dos responsáveis, essas informações serão utilizadas pelos tomadores de decisão para estabelecer o rumo da corporação (2003, p.1).

A informação que o engenheiro social deseja pode não ter valor para uma organização, mas para o atacante pode ser uma boa pista para encurtar sua rota de ataque e sucessivamente cumprir sua estratégia. Exemplo: documentos que são jogados no lixo sobre algum projeto de algum software que a empresa não realizou ou algum esboço de um novo produto.

"Grande parte das informações aparentemente inócuas de posse de uma empresa é cobiçada por um atacante da engenharia social porque ela pode ter um papel vital em seu esforço de se revestir de credibilidade" (Mitnick e Simon, 2003, p.14).

Quando a informação é confidencial[1] e uma única pessoa é responsável por mantê-la segura o ataque do engenheiro social é facilitado, ou seja, os equipamentos responsáveis por cooperar com a segurança da informação são praticamente inúteis, pois o alvo final dos engenheiros sociais são pessoas e não equipamentos e softwares.

De acordo com Mann:

> O tipo de informação que é guardada somente por indivíduos essenciais pode dificultar a segurança, pois seu controle é limitado. Um engenheiro social está a somente um truque de distância de obter a revelação dessas informações, pois controles físicos e eletrônicos de acesso não podem ser aplicados (2011, p.23).

2.2. Vendedores de segurança da informação

Os vendedores de segurança da informação só pensam em lucrar, não trazem muitas soluções para melhorar a proteção do ativo[2] mais importante das empresas, portanto, não demonstram tanta preocupação nos colaboradores das organizações.

De acordo com Mann:

> O negócio da segurança da informação é dominado pelos fornecedores de hardware e software de segurança de T.I. Apesar de os produtos desses fornecedores terem importância (alguns podem até melhorar sua segurança!), eles não resolvem sua maior fraqueza – as pessoas (2011, p.28).

As organizações precisam entender que as pessoas são responsáveis pelo resguardo da informação e quando é somada ao conhecimento traz a inovação, não adianta gastar em sistemas mais robustos se não protegerem as pessoas, ou seja, as empresas gastam muito em equipamentos e muito pouco com os funcionários e estes estão na mira dos ataques envolvendo engenharia social. Não vai fazer diferença na segurança da informação se o foco das organizações for mais a parte técnica do que o lado humano.

Segundo Ferreira:

> "[...] Todo profissional de segurança da informação sabe que o elo mais fraco é o ser humano. Não adianta você investir milhões em equipamentos e sistemas de segurança, sendo que, em apenas uma ligação é possível obter uma credencial para acessar o sistema da empresa" (2015, p.1).

O hardware e software que as organizações compram não surtem efeito positivo se não tiverem consciência que os funcionários são importantes. O fato de o engenheiro social explorar esse lado mais fraco da segurança é porque as empresas prezam pela integridade de seus equipamentos que ajudam na confidencialidade da informação e não pelo lado humano.

> Os tecnologistas experientes têm desenvolvido soluções de segurança da informação para minimizar os riscos ligados ao uso dos computadores, mas mesmo assim

[1] Confidencial: informação disponível somente para pessoa autorizada.
[2] Ativo: tudo o que é importante para as empresas. Exemplo: pessoas, equipamentos e etc.

deixaram de fora a vulnerabilidade mais significativa: o fator humano. (Mitnick e Simon, 2003, p.7).

2.3. Áreas de riscos

O engenheiro social pode facilmente tentar enganar os funcionários de uma determinada empresa fazendo com que os mesmos forneçam diversas informações importantes ou até se infiltrar em áreas especificas, consequentemente visando o dinheiro pela venda do ativo ou o vazamento para concorrentes e outras inúmeras possibilidades, é comum pessoas não autorizadas usarem disfarces ou omitirem a verdadeira função para entrar em algum lugar sem ser notado pelos guardas de segurança da informação que ficam do lado de dentro em um perímetro mais limitado ou pelos seguranças que vigiam o lado de fora, outro meio seria enganar o suporte de informática utilizando a persuasão para obter login e senha de algum sistema, as latas de lixos perto desses lugares são uma fonte a mais a ser explorada, portanto, dentro do ambiente de trabalho é preciso ter responsabilidade em não divulgar as informações sem antes confirmar se quem a está solicitando é realmente um funcionário, e, também entender a maneira correta e mais eficiente de descartar o ativo quando não tiver mais utilidade para os planos da organização, se tem permissão para acessar e se faz parte daquela área (TECHNET, 2006).

A tabela 1 mostra as áreas de riscos e as táticas utilizadas pelos atacantes. Existem várias áreas de riscos dentro das organizações, o engenheiro social está sempre buscando uma tática para fazer mais vítimas (POPPER e BRIGNOLI, 2003):

Área de risco	Tática do engenheiro social
Suporte de Informática	Realizar um telefonema para enganar com o objetivo de conseguir algumas informações importantes.
Entrada de edifícios	Ir com um disfarce para conseguir entrar sem levantar suspeitas dos seguranças ou de outros colaboradores.
Escritórios	Procurar arquivos que possam contribuir em um futuro ataque.
Sala dos servidores	Colocar softwares espiões para monitorar as atividades da organização.
Central telefônica	Grampear os telefones para ouvir as conversas.
Internet e Intranet	Colocar softwares para obter as senhas dos colaboradores.
Depósito de lixo	Procurar no lixo documentos com o objetivo de obter alguma informação.

Tabela 1: Áreas de riscos e táticas do engenheiro social
Fonte: POPPER e BRIGNOLI, 2003, p.8

2. TIPOS DE ENGENHEIROS SOCIAIS

Os engenheiros sociais estão sempre buscando um jeito mais fácil de encontrar vulnerabilidades[3] nos colaboradores sem muito conhecimento ou desmotivados ex-funcionários e até hackers que desejam se vingar, portanto, é mais comum nesses ambientes mais sensíveis acontecer traição, ou seja, o funcionário x pode ser comprado por um concorrente ou deixar de ser confiável (MANN, 2011).

Os principais tipos de intrusos e objetivos podem ser estudantes, crackers representantes comerciais, executivos, espiões, contadores, corretores de valores, ex-funcionários, funcionários e vigaristas (POPPER e BRIGNOLI, 2003).

A primeira façanha de Kevin foi descobrir com um motorista de ônibus como funcionava o processo de furos nos bilhetes, em seguida, encontrou um furador e alguns bilhetes que não haviam sido usados nos lixos dos terminais de ônibus, o ato lhe rendeu viajar por Los Angeles sem pagar nenhum centavo (ARRUDA, 2011).

A engenharia social foi muito bem aplicada por Kevin e este enviou arquivos confidenciais (continham informações sobre as vulnerabilidades do sistema financeiro do país) para o congresso americano, a façanha foi tão simples que não foi necessário utilizar técnicas mais avançadas, ou seja, foi necessária só uma mera abordagem pessoal para obter êxito (MANN, 2011).

De acordo com Mann:

> Um dos hackers mais famosos até hoje foi Kevin Mitnick. Ele ganhou mais notoriedade quando foi preso sem julgamento, nos Estados Unidos, e pelas coisas realmente ridículas ditas sobre o perigo que ele era para a sociedade do que por suas explorações reais de hackeamento (2011, p.64).

Além de trabalhar como lavador de pratos também era hacker, Abdallah utilizou engenharia social para cometer fraudes, cerca de US$80 milhões foram roubados, conseguiu informações em uma lista da revista forbes e esta havia publicado em uma edição as 400 pessoas mais ricas dos EUA, com essas informações Abdallah foi atrás de suas vítimas, enganou até os bancos para conseguir roubar os números de vários cartões de créditos (INÁCIO, 2013).

Utilizou um computador de uma biblioteca e um celular para enviar e-mails aos bancos para obter dados sobre os alvos como Steven Spielberg e George Lucas, consequentemente, teve a oportunidade de realizar o acesso a contas de famosos que eram clientes dos bancos Goldman Sachs, Bear Stearns e Merrill Lynch. Os investigadores rastrearam uma encomenda no valor de US$ 25 mil de dispositivos que clonavam cartões e se disfarçaram de entregadores para prender Abdallah (ARRUDA, 2011).

[3] Vulnerabilidades: alguma fraqueza de alguma coisa, se for explorada causará prejuízos.

Daniel, um engenheiro social não muito conhecido, um espião de concorrentes, foi responsável por pegar o banco de dados de uma organização. Não tinha amizade com nenhum colaborador da empresa alvo, usou um disfarce de investidor internacional para conseguir passar pela segurança do local sem levantar suspeitas, em seguida entrou em um elevador e deixou cair um cd e este tinha uma mensagem (por favor, não abra, fotos comprometedoras), por curiosidade alguém pegou esse cd e colocou no computador para ver os arquivos, depois de algum tempo Daniel já tinha acesso a todas as informações da empresa inclusive o banco de dados, portanto, um ataque desse nível pode parecer fácil, mas não é bem assim, a abordagem pessoal é um dos ataques mais difíceis ainda mais pelo fato de entrar em um local desconhecido (DELGADO, 2012).

2.1. Tipos de ataques

Os ataques podem ser realizados por diversos tipos de técnicas dentro ou fora do ambiente corporativo, existe uma regra que deve ser adotada pelos engenheiros sociais, é sempre agir de acordo com tipo de ataque, por exemplo, o uso de um disfarce apropriado para adentrar em um local da empresa não autorizado (MANN, 2011).

A figura 5 representa o ciclo de ataque de um engenheiro social, são divididos em quatro fases e estas são essenciais para o ataque se concretizar (BRASIL, 2014).

Figura 1: Ciclo de ataque de engenharia social
Fonte: Brasil, 2014, p.1

Na primeira fase, o engenheiro social consegue o máximo de informações possíveis da suposta vítima mais vulnerável, na segunda fase, começa o relacionamento de amizade ou até namoro com o alvo, na terceira fase, é feita a obtenção de mais informações para poder iniciar o ataque e na quarta e última fase se inicia o ataque (MARTINS, 2014).

Phishing é uma técnica de ataque indireto muito utilizado pelos engenheiros sociais, o objetivo é pescar informações da vítima. Quando o atacante envia um e-mail com um arquivo anexado ou algum link de algum site falso com um tipo de malware para o alvo e, em seguida a vítima recebe o e-mail e clica para ler as informações do arquivo, consequentemente morde

a isca, um software malicioso é instalado no computador, esse tipo malware coleta informações importantes que podem servir para o agressor dar continuidade ao ataque (MÜLLER, 2012).

Segundo uma pesquisa realizada pela empresa McAfee[4] (2013, apud UOL SEGURANÇA ONLINE, 2014), 80% das pessoas clicaram em ao menos um dos e-mails, se um único funcionário abrir o e-mail e clicar no arquivo sem saber sua origem, consequentemente todo o sistema da empresa pode ser comprometido. As áreas de recursos humanos e contabilidade são mais visadas pelos atacantes.

A figura 6 mostra um exemplo de um e-mail que foi enviado com phishing para um rh, nesse caso a vítima excluiu porque sabia suspeitou de que era um software espião (ELPESCADOR, 2016).

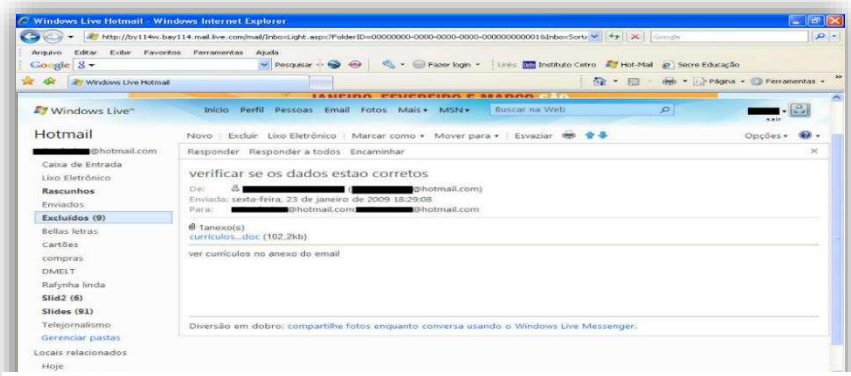

Figura 2: O envio de um e-mail malicioso pode resultar em perdas incalculáveis
Fonte: ElPescador, 2016, p.1

Na abordagem pessoal, o atacante faz uma visita para a empresa que deseja realizar o ataque fingindo ser um fornecedor, um funcionário, amigo de um colaborador, prestador de serviços ou um investidor estrangeiro e etc. Utilizando a habilidade para enganar os funcionários o engenheiro social passa pela recepção, pelos seguranças ou guardas de segurança e consegue entrar na sala onde fica localizado o data center[5] onde inevitavelmente buscará por informações confidenciais (RAFAEL, 2013).

Outra técnica de phishing, porém não é realizada por e-mail e sim pelo envio de uma mensagem (SMS ou MMS) para o número do colaborador. O ataque de smishing consiste em uma mensagem que contém um texto de urgência e um link, se o mesmo for clicado redireciona o alvo para uma página, em seguida instala um malware no celular com a função de coletar os

[4] McAfee: empresa desenvolvedora de antivírus
[5] Data centers: é o local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa.

dados, outra possibilidade é o link redirecionar o alvo para um site falso no qual são requeridos os dados pessoais ou dados corporativos (BESSA, 2015).

Telefones IP: dispositivos que tem aparentam ser um telefone comum, porém não são, usam um roteador para poderem realizar um telefonema. Computador para computador: existem softwares gratuitos que realizam ligações pelo voip, só é preciso utilizar um microfone e um software, por exemplo: skype. Smartphones: existem vários softwares para dispositivos mobile que fazem esse tipo de ligação. Exemplo: skype, icq, google talk e etc. (LUIZ, 2013).

O Vishing é uma técnica onde o atacante faz uma ligação para o alvo utilizando voz sobre ip. Exemplo: o engenheiro social escolhe como alvo um técnico de suporte de uma empresa X, em seguida, o atacante liga para esse suposto alvo e diz que não consegue acessar o sistema Z porque não lembra o login e senha, em seguida o alvo passa as informações que foram requeridas para o engenheiro social.

> No Voice Phishing, também apelidado de Vishing, você em geral receberá uma ligação explicando que uma transação bancária sua não foi bem sucedida, ou que você tem problemas com alguns dados, além de qualquer outra mentira que torne possível a coleta dos seus dados (Fonseca, 2009, p.1).

A empresa CriticalX empreendedora de T.I (Tecnologia da Informação) fornece alguns sistemas para outras organizações, o PeopleEasy é um dos sistemas desenvolvidos pela CriticalX para a área de recursos humanos. A empresa BankY é um cliente da CriticalX, o foco dos hackers era conseguir informações para encurtar o caminho até o alvo principal, o BankY. Uma pessoa do grupo HackerZ telefonou para o suporte técnico da CriticalX e se identificou com o nome Sarah, o nome do técnico era JohnnyT, ao decorrer da conversa foi possível descobrir informações sobre o responsável por administrar o banco de dados, descobriu-se que o próprio técnico que estava prestando ajuda tinha acesso completo de administrador ao banco de dados. Sarah havia dito que não estava conseguindo acessar o sistema de rh PeopleEasy, em seguida, pediu a JohnnyT para enviar uma planilha com todas as informações sobre os funcionários do BankY, depois, no e-mail de Sarah várias planilhas chegaram, além das informações dos funcionários que estavam no arquivo, os registros das contas bancárias dos colaboradores estavam dentro da planilha, portanto o ataque foi realizado com sucesso (MANN, 2011).

A técnica conhecida pelo nome de surfar sobre os ombros de outra pessoa, o engenheiro pode entrar em uma área da empresa sem autorização para roubar informações utilizando a

observação ou algum equipamento que possa filmar o momento em que um determinado colaborador esteja digitando algo. Exemplo: login e senha (ARRUDA, 2011).

"A técnica de olhar pelo ombro (Shoulder Surfing) é basicamente aquele famoso "espiar" o que o outro está fazendo, o que está digitando, e ficar atento a detalhes do trabalho alheio" (Inácio, 2016, p.1).

Tailgate, dentro da organização o colaborador pode ser gentil demais e acabar segurando a porta para outro entrar em áreas onde o acesso é controlado, essa pessoa pode não fazer parte do ambiente, ou seja, pode ser o engenheiro social se infiltrando graças à gentileza de alguns funcionários.

> Esse método de ataque, muitas vezes, é decorrente do excesso de cortesia dos funcionários. Quantas vezes você manteve a porta aberta porque vinha outra pessoa logo atrás de você que também iria entrar no mesmo recinto? Isso em empresas que usam leitor de cartão como forma de validação para que a porta se abra, mantê-la aberta pode ser um erro fatal, pois, essa pessoa pode ser alguém com intenções maliciosas e que acabou de fazer uso do tailgate para entrar sem permissão no recinto (Inácio, 2016).

A figura 8 mostra uma imagem de uma pessoa x entrando porque o y não fechou a porta assim que entrou no local (INÁCIO, 2016).

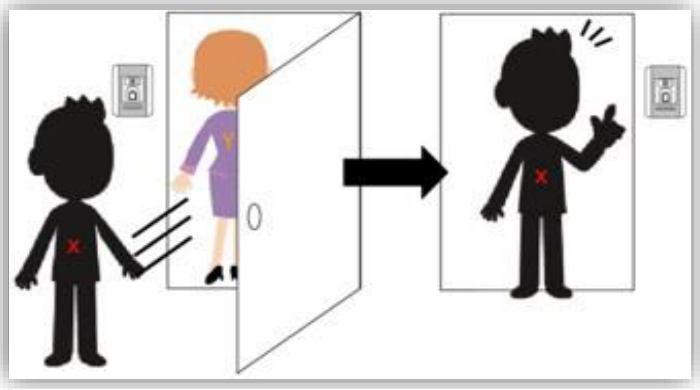

Figura 3: O colaborador deixa a porta aberta para outra pessoa que está atrás entrar.

O engenheiro social pode se aproveitar do lixo que é descartado pelas empresas para buscar informações confidenciais, por exemplo, nome dos principais clientes, nome dos colaboradores, números de contatos dos fornecedores, e-mails e até informações sobre um projeto que não teve sucesso para a organização (RAFAEL, 2013).

Hoje em dia é possível obter informações sobre as empresas, funcionários e de outras pessoas através da internet e por meio das redes sociais, o engenheiro social utiliza essa técnica para escolher um alvo mais adequado para poder estudá-lo e também porque é fácil de conseguir informações sobre o endereço da organização alvo (RAFAEL, 2013).

A engenharia reversa é um ataque mais difícil de obter informações, requer muita pesquisa e muito preparo. Esse ataque é composto por três fases, primeira fase é a sabotagem onde o engenheiro social derruba algum sistema da empresa fazendo com que seja necessário chamar algum técnico, na segunda fase o atacante inventa uma personalidade de autoridade, faz um anúncio para a empresa que sofreu o ataque e diz que sabe resolver o problema, na terceira e última fase caso a empresa faça contato o atacante vai até o local e solicita informações para os colaboradores sobre o sistema e outras informações confidenciais, em seguida, o engenheiro social resolve o problema e consegue atingir objetivo sem ser notado por outros funcionários (GRANGER, 2001, tradução nossa).

2.2. Medidas para mitigar os ataques

As medidas não garantem totalmente a segurança das informações das empresas, ou seja, não existe algo completamente seguro que possa garantir a confidencialidade das informações, enquanto tiver pessoas sempre haverá vulnerabilidades que podem ser exploradas. As medidas estão contidas na política de segurança da informação (MURBACH, 2015).

Uma Política de Segurança da Informação (PSI) constitui-se de diretrizes, normas e procedimentos necessários para garantir que todos os colaboradores, fornecedores e parceiros cumpram o que for estabelecido, ou seja, são regras que devem ser seguidas com seriedade. É um documento desenvolvido por uma comissão formada por vários funcionários de diversas áreas da empresa (SANTANA, 2009).

As principais medidas para diminuir os ataques estão contidas na PSI, algumas destas a serem abordadas são:

Na segurança física, a entrada dos colaboradores ou de outras pessoas em locais com informações confidenciais só deve ser permitida mediante a autorização, é fundamental os guardas de segurança realizarem o monitoramento constante, caso haja algum suspeito será necessário reportar para o responsável por cuidar da segurança da informação, adicionar sistemas de biometria ou guardas posicionados em um perímetro mais reduzido para tentar inibir possíveis infratores. Em segurança lógica, o controle de acesso é importante para evitar que pessoas indevidas acessem informações sigilosas sem permissão e esta pode ser um processo de criação, remoção, alteração de contas e execução de programas maliciosos que causem transtornos e prejuízos incalculáveis para a organização, utilizar criptografia em todos os arquivos confidenciais. No treinamento e conscientização é de extrema importância a empresa explicar para todos os colaboradores que a informação é um ativo fundamental e

valioso. Fazer uma palestra para todos os funcionários sobre as técnicas de ataques de engenharia social, aplicar um treinamento ou uma simulação de ataque para que seja possível medir o desempenho da organização em identificar ou amenizar os ataques (INÁCIO, 2013).

Em mesa limpa, deixar os documentos com informações confidenciais guardados em uma gaveta com chave, os computadores deverão ser bloqueados quando o funcionário sair do local de trabalho, não deixar senhas fixadas em um papel em baixo do teclado, não anotar as senhas em papéis. Utilizar um fragmentador de papel nos escritórios ou contratar uma empresa especializada que faça o serviço de destruição dos arquivos das mídias removíveis ou dos arquivos do disco rígido dos computadores antigos. (SAFE WAY, 2016).

No processo de admissão ou demissão os funcionários deverão assinar o termo de responsabilidade para coibir a divulgação de informações confidenciais, não compartilhar senhas com outros funcionários, caso alguma informação seja vazada o responsável irá pagar uma multa (Pinheiro, 2011).

A classificação da informação tem o objetivo de discernir os níveis de confidencialidade para proteger o ativo, o nível de classificação da informação vai depender do tamanho da empresa. A informação pode ser classificada em:

Pública: a informação pode ser vista por todos sem nenhum problema. Interna: Somente pessoas de dentro da empresa podem acessar a informação, mesmo se alguém não autorizado conseguir acesso indevido não causará prejuízos. Confidencial: somente para alguns funcionários, o vazamento deste tipo de informação pode causar prejuízo. Secreta/Restrita: totalmente confidencial somente visível para uma quantidade pequena de pessoas, esse tipo de informação é fundamental para a sobrevivência das empresas (MÜLLER, 2014).

CONSIDERAÇÕES FINAIS

Em virtude dos fatos mencionados nesse artigo, pode-se ter uma noção da preciosidade da informação para as organizações, investimentos somente em equipamentos técnicos não surtem resultados positivos se o lado humano for ignorado. Por isso, o engenheiro social visa explorar os sentimentos das pessoas com a ajuda de técnicas específicas.

Portanto, corporações que deixavam a informação confidencial somente com um colaborador estavam mais propensas de sofrer os ataques. Pode-se notar que a porcentagem de empresas que priorizam a segurança desse ativo é equilibrada, porém, quem não deixou bem

clara a política de segurança da informação em conjunto aos treinamentos e conscientizações sobre os perigos da engenharia social teve perdas financeiras muito altas.

Conclui-se que as pessoas são as mais frágeis no ambiente corporativo e que nenhuma organização está completamente segura mesmo se for aplicado medidas para amenizar esses incidentes, pois sempre haverá funcionários com informações importantes e engenheiros sociais com o interesse em obter esse ativo, ou seja, nada nesse mundo é 100% seguro.

REFERÊNCIAS BIBLIOGRÁFICAS

Amcham. 2010. **“PWC: 50% das empresas investem em segurança da informação”**. Disponível em: <http://www.amcham.com.br/business-in-growth/noticias/pwc-50-das-empresas-investem-em-seguranca-da-informacao>. Acesso em: 15/01/2020.

Arruda, Felipe. 2011. **“Engenharia social: o malware mais antigo do mundo”.** Disponível em: <http://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm>. Acesso em: 07/01/2020.

Benetti, Ticiano. 2015. **“Segurança da informação – confidencialidade, integridade e disponibilidade (CID)”**. Disponível em: <https://www.profissionaisti.com.br/2015/07/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid/>. Acesso em: 29/01/2020.

Bessa, Beatriz. 2015. **“Phishing”**. Disponível em: <http://pt.slideshare.net/BiaBessaa/phishing-1?qid=2ae98d3a-58bc-461d-970f-00b8d1d96a4b&v=&b=&from_search=3>. Acesso em: 05/01/2020.

Brasil, Márcio. 2014. **"O que é social engineering".** Disponível em: <http://www.marciobrasil.net.br/dicas/o-que-e-social-engineering.html>. Acesso em: 01/02/2020.

Delgado, Yuri. 2012. **“Hackers, crackers, Engenharia Social e a ignorância humana”**. Disponível em: <http://www.yuridelgado.com.br/11/hackers-crackers-engenharia-social-e-a-ignorancia-humana>. Acesso em 01/02/2020.

Diogenes, Yuri. 2011. **"Os atuais riscos da Engenharia Social - Revista Infra Magazine 3".** Disponível em: <http://www.devmedia.com.br/os-atuais-riscos-da-engenharia-social-revista-infra-magazine-3/22931>. Acesso em: 01/02/2020.

ElPescador. 2016. **“Recursos Humanos: uma área muito sensível a ataques de phishing”**. Disponível em: <https://www.elpescador.com.br/blog/index.php/recursos-humanos-uma-area-muito-sensivel-a-ataques-de-phishing/>. Acesso em: 01/02/2020.

Ferreira, Marcos. 2015. **"O que é engenharia social? 6 dicas para se proteger das armadilhas"**. Disponível em: <***https://www.trustsign.com.br/blog/o-que-e-engenharia-social-6-dicas-para-se-proteger-das-armadilhas/index.html***>. Acesso em: 15/05/2016.

Fonseca, Willian. 2009. **"Já ouviu falar em voice phishing? ".** Disponível em: <http://www.tecmundo.com.br/antivirus/1784-ja-ouviu-falar-em-voice-phishing-.htm>. Acesso em: 06/06/2016.

Granger, Sarah. 2001. **"Social Engineering Fundamentals, Part I: Hacker Tactics"**. Disponível em: <http://online.securityfocus.com/infocus/1527>. Acesso em 09/06/2016.
Inácio, Sandra Regina da Luz. 2013. "Entendendo e evitando a engenharia social: protegendo sistemas e informações". Disponível em: <http://www.projetodiario.net.br/entendendo-e-evitando-a-engenharia-social-protegendo-sistemas-e-informacoes***>. Acesso em: 01/02/2020.***

Inácio, Sidnei. 2016. **"Engenharia social – tipos de ataques".** Disponível em: <https://www.linkedin.com/pulse/engenharia-social-tipos-de-ataques-sidnei-in%C3%A1cio>. Acesso em: 07/01/2020.

LAUDON, Kenneth C. e LAUDON, Jane P. **"Sistemas de Informações Gerenciais"**. Ed. Prentice Hall; São Paulo, 2007.

Luiz, André. 2013. **"Voip: o que é? Como funciona?"**. Disponível em: <http://www.tekimobile.com/funcionamento-voip/>. Acesso em: 07/06/2016.
MANN, Ian. **"Engenharia Social".** Ed. Blucher, 1° edição, 2011.

Martins, Rodrigo. 2014. **"Engenharia social"**. Disponível em: ***<https://atitudereflexiva.wordpress.com/2014/08/26/engenharia-social/>. Acesso em: 30/01/2020.***

MITNICK, Kevin D.; SIMON, William L. "A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação". São Paulo: Pearson Education, 2003.

Murbach, Danilo. 2015. "Dicas simples para promover a segurança de sua empresa". Disponível em: <http://asteriks.com.br/infraestrutura/dicas-simples-para-promover-a-seguranca-de-sua-empresa/>. Acesso em: 01/02/2020.

Pinheiro, Alexander. 2011. **"Termo de compromisso, sigilo e confidencialidade #2"**. Disponível em: <http://www.tiespecialistas.com.br/2011/11/termo-de-compromisso-sigilo-e-confidencialidade-2/>. Acesso em: 01/02/2020.

Popper, Marcos Antonio; Brignoli, Juliano Tonizetti. 2003. **"Engenharia social um perigo eminente"**. Disponível em: <http://docplayer.com.br/3991308-Engenharia-social-um-perigo-eminente.html>. Acesso em: 01/02/2020.

Rafael, Gustavo de Castro. 2013. **"Engenharia social: as técnicas de ataques mais utilizadas"**. Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em: 07/01/2020.

Safe Way. 2016. **"Sua equipe está preparada para os ataques de engenharia social?".** Disponível em: <http://safewayconsultoria.com/engenharia_social/>. Acesso em: 15/06/2016.

Santana, Lucas L. 2009. **"Como elaborar uma política de segurança da informação (parte I)"**. Disponível em: <https://www.profissionaisti.com.br/2009/06/como-elaborar-uma-politica-de-seguranca-da-informacao-parte-i/>. Acesso em: 14/01/2020.

Svaiter, David Ben. 2015. **"Qual o valor da Informação?".** Disponível em: <https://www.linkedin.com/pulse/qual-o-valor-da-informa%C3%A7%C3%A3o-david-ben-svaiter?forceNoSplash=true>. Acesso em: 09/01/2020.

TECHNET, 2006. **"Como proteger as pessoas de dentro da empresa contra ameaças de engenharia social".** Disponível em: <https://technet.microsoft.com/pt-br/library/cc875841.aspx>. **Acesso em: 14/01/2020**..

Torres, Sthefane. 2015. **"6 casos reais de falhas de segurança em grandes empresas".** Disponível em: <https://www.trustsign.com.br/blog/6-casos-reais-de-falhas-de-seguranca-em-grandes-empresas/index.html>. Acesso em: 14/01/2020.