Revista Inteligência Competitiva
http://www.inteligenciacompetitivarev.com.br/ojs/index.php/rev
ISSN: 2236-210X
DOI 10.24883

V. 9, N. 1, JAN./MAR. 2019

O USO DE ATAQUES DIRETOS E PESSOAIS DA ENGENHARIA SOCIAL PARA A OBTENÇÃO DE INFORMAÇÕES DE UMA CORPORAÇÃO

THE USE OF DIRECT AND PERSONAL ATTACKS FROM SOCIAL ENGINEERING TO OBTAIN INFORMATION FROM A CORPORATION

Eurico Dos Santos Moreira.
Faculdade Unyleya. Brasil.
✉urico.moreira.cascavel@gmail.com

ARTIGO

Editor
Alfredo Passos
profdrpassos@gmail.com

Como referenciar – ABNT

MOREIRA, Eurico dos Santos. O uso de ataques diretos e pessoais da engenharia social para a obtenção de informações de uma corporação. **Revista Inteligência Competitiva**, v. 9, n. 1, p. 55-72, jan./mar. 2019.

RECEBIDO EM: 21/12/2017
APROVADO EM: 27/11//2018

Rua Pe. Guilherme Pompeu, nº1,
Centro- Santana de Parnaíba
06501-055 - São Paulo - Brasil

Resumo: O objetivo geral do trabalho é conhecer como os ataques diretos e pessoais da Engenharia Social se relacionam com a obtenção de informações de uma Corporação. Buscando a construção do conhecimento por parte do leitor, têm-se como objetivos específicos: a definição de Engenharia Social, as formas de atuação de um engenheiro social, definição e características de ataques de forma direta e pessoal, o fator humano e as possíveis vulnerabilidades que uma corporação diante deste tipo de ameaça. Por meio de uma revisão bibliográfica qualitativa foi realizado uma pesquisa na literatura existente, monografias acadêmicas e publicações de especialistas e empresas da área de SI. Esperando-se assim, poder contribuir no aprimoramento dos Análises de Riscos e procedimentos de segurança de uma corporação.

Palavras Chaves: Engenharia social. Segurança da informação. Vulnerabilidade. Análise de risco.

Abstract: The general objective of the paper is to know how the direct and personal attacks of Social Engineering are related to obtaining information of a Corporation. Seeking to construct the knowledge by the reader, the specific objectives are: the definition of Social Engineering, the ways of social engineer's attacks, the performance of a social engineer in a direct and personal way, the human factor and the vulnerabilities that a corporation may be exposed by an attack of social engineering in a direct and personal way. Through a qualitative bibliographical review a reaserch was carried out in the existing literature, in academic monographs and specialists publications and companies in the SI area. It is hoped to contribute to the improvement of the Risk Analysis and safety procedures of a corporation.

Keywords: Social engineering. Information security. Vulnerabilities. Risk analyses.

1 INTRODUÇÃO

Desde o início da formação de uma sociedade organizada já se destacava, de forma negativa, aqueles indivíduos que utilizavam de suas expertises para aproveitarem-se da inocência e confiança das pessoas para obter vantagens de forma desleal e ilícita. Os praticantes desta categoria de ilícito ganharam um apelido em nosso país de "171", devido ao artigo do Código Penal Brasileiro (CP) que tipifica o crime de estelionato. Definido no CP como: "Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento." (BRASIL, 1940).

Segundo Siqueira, a partir da década de 90, a informação tornou-se uma vantagem competitiva e a ter uma importância de sobrevivência e prosperidade para qualquer organização. Tornou-se objeto de grande valor agregado e atrativo a nova geração de algozes que se aprimoraram utilizando além da inteligência e astúcia, também as tecnologias da informação (TI) como meio de obtenção de informações restritas. A informação e o conhecimento tornaram-se produtos econômicos na competitividade empresarial, aumentando a necessidade de proteção, controle e manutenção em TI de forma plena e organizada (2005 apud BALDIN, 2007). Os investimentos aplicados em segurança de TI estão sendo volumosos, buscando evitar a "perda" dos ativos das organizações de qualquer nível ou setor empresarial.

Contudo, Mitnick (2003) alerta que os especialistas têm desenvolvido soluções de segurança da informação para minimizar os riscos ligados ao uso dos computadores, mas mesmo assim deixaram de fora a vulnerabilidade mais significativa: o fator humano. E que apesar do nosso intelecto, nós humanos — você, eu e todas as outras pessoas — continuamos sendo a ameaça mais séria à segurança do outro. Ele nos apresentou o termo: Engenheiro Social como sendo aquela pessoa ardilosa, inteligente que somada aos conhecimentos técnicos continua sendo um fator de risco, muitas vezes fora do foco de nossos especialistas em segurança da TI.

De acordo com Sêmola (2003, apud BALDIM, 2007), muitos empresários não conseguem "enxergar" a complexidade que está envolvida na segurança da informação. Possuem uma deficiência chamada por ele de "Visão de Iceberg" (a porção de gelo fora da linha da água corresponde apenas à 1/5 de todo o bloco de gelo que permanece submerso). Esta visão distorcida associa, de forma leviana, apenas aos riscos de redes, computadores, vírus, harckers e Internet. Contudo, existem outros fatores interelacionados entre segurança patrimonial e da informação que são primordiais no contexto empresarial.

Segundo a pesquisa da Daryus (2014), mais de 40% das falhas à Segurança da Informação não está associada à tecnologia, mas sim em torno de usuários e a maneira na qual os dados, informações e sistemas são utilizados ou guardados nas organizações. Destes mais de 40% das falhas à Segurança da Informação é possível de que boa parte estejam ligados a ataques de engenheiros sociais, e mais especificamente por meio de ações diretas e pessoais. Os ataques de engenheiros sociais na forma direta e pessoal é pouco explorado e exemplificado dentro da Segurança em TI, talvez porque quando estas técnicas são bem empregadas pela engenharia social não deixam rastros ou se imputa a culpa a terceiros.

Neste contexto, esta pesquisa pretende apresentar e conhecer este tipo de ameaça silenciosa e pouco considerada nas literaturas de Análise de Riscos Corporativos. Será abordado no primeiro capítulo uma apresentação do que é Engenharia Social e suas formas de atuação, no segundo capítulo será abordado especificamente o Ataque Direto e Pessoal de um Engenheiro Social passando pelo Fator Humano, alvo deste tipo de ação. E por fim, no terceiro capítulo, pontuar algumas possíveis vulnerabilidades de uma Corporação diante de um ataque da engenharia social na forma direta e pessoal.

2 A ENGENHARIA SOCIAL E SUAS FORMAS DE ATUAÇÃO

2.1 O QUE É ENGENHARIA SOCIAL?

O termo engenharia social, dentro da Segurança da Informação, nasceu no início da década de 1990 na forma de atuação do então mais famoso hacker, Kevin Mitnick. Para Mitnick (2003), engenharia social é uma técnica de ataque que explora a vulnerabilidade humana, por intermédio da persuasão e enganação para conseguir informações se utilizando da tecnologia ou não. A partir da sua história de vida e de seus livros, outros autores trataram a Engenharia Social na mesma linha de pensamento.

Gartner (2002, apud BALDIM, 2007) diz que a Engenharia Social envolve mais a manipulação de pessoas do que a utilização dos meios tecnológicos para burlar um sistema de segurança da informação. Atua por meio de habilidades técnicas e interpessoais para encontrar falhas na segurança empresarial, assim se apoderando de informações sensíveis.

No ano de 2011, em seu livro dedicado exclusivamente a Engenharia Social Ian Mann resumiu como: "Manipular pessoas, enganando-as, para que forneçam informações ou executem uma ação" (2011, p. 19). E mais recentemente, Eduardo Vasconcelos se "atreveu" a exprimir a sua definição: "Coagir pessoas a executar ações ou aproveitar-se de ações livremente executadas para conseguir acesso a informações ou áreas reservadas, físicas ou virtuais" (2017).

Para Peixoto (2006), uma das dificuldades mais complexas enfrentada pelos gestores de segurança, são as vulnerabilidades exploradas pela engenharia social. Estas vulnerabilidades estão diretamente relacionadas as brechas exploradas na complexidade do ser humano, se valendo de fraquezas sociais, psicológicas ou comportamentais. Tais brechas que fragilizam a segurança de uma corporação nas áreas de tecnologia, física, recursos humanos. Ou seja, em todo o sistema organizacional.

Por estes conceitos, apresentados ao longo de mais de 15 anos, se observa que todos convergem para o ser humano como meio essencial para o êxito das ações da engenharia social. Entretanto, as tecnologias tem sido cada vez mais uma aliada dos engenheiros sociais como ferramentas que lhe dão facilidades e segurança.

2.2 AS FORMAS DE ATUAÇÃO DE UM ENGENHEIRO SOCIAL

Mitnick (2003, p. 11), no prefácio de seu livro: A arte de enganar, nos diz que: "Quando você combina uma inclinação para enganar as pessoas com os talentos da influência e persuasão, você chega ao perfil de um engenheiro social".

Em seu artigo, Cássio Bastos Alves (2010, p. 15) classificou:

> Os ataques de engenharia social podem ser divididos em dois grupos: Os ataques diretos: Como o próprio nome já diz, são aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas, fax e até mesmo pessoalmente. Este exige do engenheiro social, um planejamento antecipado e bem detalhado, além de um segundo plano para caso o primeiro não dê certo, além de muita criatividade e articulação para que o plano seja bem-sucedido. Os ataques indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir como, por exemplo, vírus, Cavalos de Troia ou através de sites e e-mails falsos para assim obter informações desejadas. (grifo nosso)

Mann (2011, p. 155), em seu livro define duas variáveis de proteção contra a engenharia social: "Resistência Pessoal: capacidade dos indivíduos de detectar um ataque e resistir a ele; e Resistência Sistêmica: capacidade do sistema de informação de resistir a um ataque sem contar com intervenção humana". Com estas variáveis apresentadas é possível inferir que também classifica os ataques em diretos e indiretos.

Com estes argumentos se conclui que os engenheiros sociais atuam, basicamente, de duas formas:

- Direta: na qual o ofensor age tendo contato com sua vítima se utilizando de algum meio como: telefone, lixo, cartas, salas de bate papo, ou ainda pessoalmente; e
- Indireta: que se resume na utilização de tecnologias, tais como: internet, intranet, softwares (spyware, phishing e outros). Forma na qual não "aparece", se protege atrás de perfis falsos ou oculto nas redes.

Por conseguinte, observamos que dentro dos ataques diretos ainda existe uma especificidade, a qual exige os talentos da influência e da persuasão. Requer também, destemor do engenheiro social em interagir com as pessoas e ambientes que lhe são alvos. Trata-se dos ataques pessoais:

> O engenheiro social, o qual, via de regra, tem habilidades de hacker, também tem habilidades pessoais opostas — habilidades bem desenvolvidas para usar e manipular as pessoas que permitem que ele consiga as informações de forma que você nunca acreditaria que fosse possível. (MITNICK, 2003, p. 107).

Rosa comenta que: "Os ataques podem ser realizados através dos meios de comunicação, como telefonemas, envio de mensagens via correio eletrônico, salas de bate-papo e até mesmo, pessoalmente" (ROSA et al, 2012 apud MAULAIS, 2016, p. 36). Abner Silva destaca que é imprescindível não esquecer que o engenheiro social tem como principal forma de ataque a persuasão, habilidade que consegue atingir pessoas de qualquer nível

social ou empresarial. "É por meio dela que eles nos induzem a um erro de julgamento que nos faz vê-los como pessoas confiáveis, o que obviamente não o são" (SILVA; Abner, 2010).

O engenheiro social se vale de várias ferramentas para complementar sua atuação pessoal, tais como: o telefone ou VoIP, internet, intranet, e-mail, salas de bate papo, correspondência, spyware, lixo, surfar sobre os ombros e P2P. Entretanto, Peixoto alerta:

> As artimanhas utilizadas por um engenheiro social estão sempre em constante evolução. Procuram sempre buscar algo inovador, diferente do tradicional, para conseguir atingir seus objetivos. Mas mesmo perante tais transformações e mudanças no segmento da arte de enganar, modificando ou incrementando seus ataques, o engenheiro social utiliza-se sempre de alguns aspectos clássicos de ataque. (2006, p. 7)

Esta colocação bem atual do Peixoto se observa na atuação dos Insiders. Termo recentemente criado para a atuação de funcionários, ex-funcionários ou terceirizados que agem dentro das empresas na obtenção de informações, agindo de forma direta ou implantando malwares nas redes internas.

Exemplificando um caso: em dezembro de 2013, a famosa rede de departamentos americana Target, teve 70 milhões de dados de clientes roubados. O prejuízo foi estimado em 2,5 bilhões de dólares e a venda das informações no mercado negro teria gerado um lucro aos fraudadores de 57 milhões de dólares. Segundo as investigações, foram utilizadas várias técnicas para a realização do complexo golpe. Porém, o mais emblemático e decisivo para o sucesso da investida estava nas mãos de um funcionário terceirizado de uma empresa de refrigeração, o qual possuía as credenciais de acesso a rede interna. (CARRO, 2014)

Logo, as formas de atuação de engenharia social se resumem em ataques diretos e indiretos. Sendo que nos ataques diretos ainda temos aqueles que se aplicam de forma pessoal, ou seja: acontece com o contato entre o invasor e sua vítima, ou ainda, se envolvendo com pessoas próximas como amigos, parentes ou colegas de trabalho.

O engenheiro social que atua de forma direta e pessoal necessita desenvolver e aplicar habilidades mais complexas sobre as vulnerabilidades humanas para atingir seu intento. Este tópico que se faz necessário conhecer um pouco mais a seguir.

3 O ATAQUE DIRETO E PESSOAL DE UM ENGENHEIRO SOCIAL

3.1 O FATOR HUMANO

Quando um engenheiro social planeja a execução de um ataque direto e pessoal, como meio de obter ou acessar o local onde encontrará a informação que está desejando, obrigatoriamente o seu foco será o fator humano. Pereira entende que:

> Em qualquer organização, por maior que seja a sua segurança, sempre haverá um fator de desequilíbrio chamado "fator humano". [...] Os maiores engenheiros sociais tiram proveito das fraquezas ou gostos pessoais de seus alvos para assim aproximar e conseguir alcançar seus objetivos. (PEREIRA, 2005 apud CÁSSIO, 2008, p. 31)

Silva Filho (2004 apud BALDIM, 2007) destaca que independente do hardware, software ou plataforma utilizada, o elemento mais vulnerável continuará sendo o ser humano. A vontade de ser útil, a necessidade de relacionamento e a propagação de responsabilidade, exemplificadas por Silva Filho, são algumas das características comportamentais exploradas pela persuasão dos engenheiros sociais. Mitnick, em A Arte de Enganar, relata em forma de questionamento que o próprio aprimoramento nas tecnologias reflete na vulnerabilidade do fator humano. As empresas e especialistas em TI tem aplicado muitos recursos e esforços no melhoramento das proteções técnicas, reduzindo consideravelmente as vulnerabilidades. Contudo, estes aprimoramentos têm direcionado, ainda mais, os ataques dos engenheiros sociais sobre as vulnerabilidades humanas.

Por quê? Porque o fator humano é o elo mais fraco da segurança. Com frequência, a segurança é apenas uma ilusão, que às vezes fica pior ainda quando entram em jogo a credulidade, a inocência ou a ignorância...No final, os ataques da engenharia social podem ter sucesso quando as pessoas são estúpidas ou, em geral, apenas desconhecem as boas práticas da segurança. (MITNICK, 2003, p. 3).

De acordo com McCarthy e Campbell (2003, apud CUNHA, 2008), "as pessoas são o seu melhor ativo de segurança – e a sua maior vulnerabilidade". Gartner (2002, apud BALDIM, 2007) entende que, normalmente o sucesso dos ataques da Engenharia Social porque, em alguma parte do processo, passa por uma vulnerabilidade do comportamento humano. E isto pode ocorrer a funcionários de qualquer nível ou área de atuação, acontecendo inclusive, sem a menor percepção. Em um quadro resumido, Gartner aponta seis tendências básicas de comportamento humano que geraram uma resposta positiva para os engenheiros sociais:

Quadro 1: COMPORTAMENTOS HUMANOS PARA RESPOSTA POSITIVA

Comportamento	Definição	Exemplo
Reciprocidade	Alguém é estigado e se sente obrigado a fazer algo sobre alguma coisa.	Você compra uma rodada de queijo quando eles te dão desconto.
Coerência	Certos comportamentos moldados são coerentes de uma pessoa a outra.	Se você perguntar algo e esperar, a pessoa vai se sentir obrigada a falar algo.
Aceitação social - Medo	Alguém é obrigado a fazer o que todo mundo faz.	Parar no meio de uma rua movimentada e olhar para cima; pessoas eventualmente irão parar e fazer o mesmo.
Simpatia	Pessoas tendem a dizer sim para aqueles que ele gosta ou sentem atraídos.	Bonitas modelos são usadas em publicidade
Autoridade	Pessoas tendem a escultar ou prestar atenção nos avisos de quem tem posição de autoridade.	"Quatro entre cinco médicos recomendam.."
Escassez	Se alguém está com poucos suplementos, isso se torna mais "precioso" e, portanto, mais apelativo.	Furbees ou Sony Playstation 2.

Fonte: Gartner Research, 2002 *apud* BALDIM, 2007.

MANN reforça: (2011, p. 21)

> Infelizmente, humanos **não** são tão fáceis de proteger como um servidor de rede. O comportamento humano é muito mais complexo. Fomos todos programados de maneiras infinitamente complexas e, portanto, reagiremos de maneiras diferentes às abordagens dos agressores. Fraudadores, hackers e embusteiros compreendem isso. Eles usam o conhecimento das fraquezas humanas para guiá-los na projeção de ataques novos e mais complexos. (grifo nosso)

É unânime o juízo dos especialistas aqui elencados que o fator humano é o elo mais sensível e complexo para a proteção das informações de uma corporação. Observa-se que, em algum momento de sua investida na obtenção de informações privilegiadas, se não em quase todo, o engenheiro social se valerá de uma fraqueza humana para atingir o seu intento.

3.2 COMO AGE UM ENGENHEIRO SOCIAL DE FORMA DIRETA E PESSOAL

Mitnick (2003, p. 25), que desde a adolescência já se utilizava das "técnicas" de engenharia social nas suas peripécias e aventuras, descreve em seu livro: "Sempre achei incrível como um engenheiro social habilidoso pode atingir esse objetivo com um ataque simples e direto. Como você verá, às vezes tudo o que ele precisa é simplesmente pedir as informações".

Peixoto (2004, p. 38), entende que um engenheiro social cresce alicerçado em três aspectos essenciais. Primeiro o científico, quando realiza um estudo aprofundando o que há disponível sobre o seu objeto de interesse, inclusive estudando todo o portfólio e linguajar específico. A técnica, na qual aplica seus conhecimentos em tecnologias, tais como: hardwares, eletrônica, programação e Tecnologias da Informação e Comunicações (TCI). Enfim, a arte como meio inovador, uma primordial característica para um engenheiro social na atuação direta sobre o comportamento humano.

> [...] a arte como o meio mais criativo e envolvente que o Engenheiro Social pode trazer levando em conta o senso lógico, mas, sobretudo emocional, que é muito bem explorado por esse mestre articulador das vulnerabilidades humanas.

No entendimento de Maulais (2016), uma das técnicas mais empregadas pelo engenheiro social para obter acesso a instalações, sistemas ou informações de uma corporação se dá pela forma direta e pessoal, na qual denomina "Abordagem Pessoal":

> Esta técnica consiste de o Engenheiro Social realizar uma visita na empresa alvo, podendo se passar por um fornecedor, terceiro, amigo do diretor, prestador de serviço, entre outros, no qual através do poder de persuasão e falta de treinamento dos funcionários, consegue sem muita dificuldade convencer um segurança, secretária, recepcionista a liberar acesso ao datacenter onde possivelmente conseguirá as informações que procura. (MAULAIS, 2016, p. 33)

Em 2006, a Microsoft Corporation lançou um documento orientando as pessoas de como se protegerem de ameaças da Engenharia Social dentro de uma empresa. Neste artigo se destaca que as abordagens pessoais são aplicadas de maneira simples e se prevalecendo da confiança. Segundo a Microsoft (2006, p. 11), estas seriam as abordagens que os engenheiros sociais mais obtêm êxito:

a) Intimidação: Abordagem na qual o engenheiro social se passa por uma pessoa com autoridade ou a menção de nomes de pessoas importantes, coagindo a vítima a fornecer as informações desejadas.

b) Persuasão: Técnica de influenciar as pessoas a realizarem o que o atacante deseja, explorando suas fraquezas comportamentais, tais como: a lisonja (elogios) e a piedade (vontade de ajudar).

c) Bajulação: Esta abordagem se dá através da construção de um relacionamento com um funcionário da empresa alvo angariando sua confiança. Esta bajulação pode ser direta ou indireta, ou seja, o engenheiro social adquire a simpatia de uma pessoa de confiança daquela que detém o acesso as informações e posteriormente obtendo uma confiança "transitiva".

d) Assistência: Nesta abordagem, o engenheiro social se oferece para ajudar a vítima, sendo que na maioria das vezes ele mesmo cria o problema. Através desta solidariedade fará com que a vítima disponibilize informações pessoais ou deixe-o acessar através de suas credenciais. Técnica também conhecida como Engenharia Social Reversa.

Peixoto, já na introdução de sua obra (2004, p. 5), elenca as principais ferramentas utilizadas pelo praticante da engenharia social. Entre elas está a atuação de forma direta e pessoal, que exige capacidade em interagir com as pessoas, persuadindo-as aos seus interesses.

> Pessoalmente (In Person Social Engineering) – O engenheiro social faz-se passar por alguém que na verdade ele não é. Adota toda uma encenação; e como um verdadeiro artista busca manipular a vítima de forma a ser bastante convincente no que diz. [...] Alguns recursos a favor do engenheiro social seriam: a sedução, a intimidação, a dramaticidade, a credibilidade.

Nesta especificidade de forma de atuação da Engenheira Social: direta e pessoal, podemos constatar que as "garras" do atacante exploram a fragilidade e a ingenuidade das pessoas. A habilidade de manipular o comportamento do ser humano é um aspecto basilar de um verdadeiro engenheiro social.

Faz parte de nossa formação, principalmente da cultura dos brasileiros, sermos prestativos e atenciosos. Com uma conversa bem-educada e um sorriso consegue-se abrir muitas portas. É conveniente uma certa cautela e conhecimento destas possíveis ações mal-intencionadas que qualquer pessoa ou instituição pode sofrer.

4 VULNERABILIDADES DE UMA CORPORAÇÃO DIANTE DE UM ATAQUE DA ENGENHARIA SOCIAL NA FORMA DIRETA E PESSOAL

As vulnerabilidades em um ambiente corporativo podem estar associadas a deficiências nas instalações físicas, softwares, hardwares, naturais e a humana. Com exceção das naturais, as demais são exploradas pela engenharia social nesta forma de atuação. No entendimento de Peixoto: "A engenharia social, propriamente dita, está inserida como um dos desafios (se não o maior deles) mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação." (2006, p. 36)

Conforme apresentado nos capítulos anteriores, o fator humano ocupa uma posição de grande relevância na avaliação de riscos de uma instituição, caracterizando-se a "porta frágil" dentro de departamentos

com informações sensíveis. De acordo com McCarthy e Campbell (2003, apud ANDRADE; CUNHA, 2008, p. 19), "as pessoas são o seu melhor ativo de segurança – e a sua maior vulnerabilidade".

Alguns setores e funções de uma corporação são mais suscetíveis aos ataques da engenharia social com o emprego das técnicas tradicionais, supostamente conhecidas. Contudo, tais técnicas associadas às novas tecnologias, inovações e engenhosidade dos atuais malfeitores continuam sendo empregadas com êxito. Se constata então, a necessidade de conhecer melhor as possíveis vulnerabilidades das instituições para um aprimoramento na proteção dos ativos.

4.1 TERCEIRIZADOS

A terceirização de serviços dentro de uma empresa gera economia, aumento de qualidade e diminuição de encargos empregatícios. Porém se trata de uma excelente porta de acesso a um engenheiro social, pois os terceirizados normalmente são pouco conhecidos dos funcionários efetivos devido sua rotatividade e possuem acesso às instalações.

A Microsoft Corporation (2016) nos diz que: "[...] O departamento de Recursos Humanos (RH) precisa ser tão cuidadoso com a triagem de segurança do pessoal terceirizado quanto é com relação aos funcionários efetivados."

4.2 ASSISTÊNCIA TÉCNICA INTERNA EM TI

Um atendimento eficaz e cortês por aquele especialista que realiza o suporte aos funcionários é imperioso para evitar descontentamentos e principalmente evitando que seja procurado uma ajuda externa não autorizada por algum integrante. Funcionários com dificuldades em concluir alguma tarefa, que no seu entendimento é o mais importante, acabam recorrendo a pessoas não autorizadas, muitas das vezes de fora da empresa. Para a Microsoft Corporation (2016) o atendimento interno é considerado uma defesa de primeiro nível contra-ataques de engenharia social.

4.3 LEITURA POR CIMA DOS OMBROS "SHOULDER SURFING"

De acordo com Danúbia e Jane (2008, p. 22): "[...] aquela famosa olhadinha quando o colega digita a senha no computador ao lado, pode resultar no roubo dessa informação e, consequentemente, o acesso aos e-mails, páginas pessoais e daí por diante." Uma forma simples e eficaz na obtenção de acesso aos sistemas internos. Outro exemplo seria quando um "colega" de trabalho lhe pede de forma gentil que acesse algum procedimento, o qual não possui acesso, e enquanto é realizado o acesso, simplesmente memoriza ou grava de forma discreta com o celular suas credenciais.

4.4 ACESSO A EMPRESA (RECEPÇÃO)

O controle de acesso de uma organização é uma peça importante do sistema de proteção, inclusive referente a informação. Na maioria das vezes se contrata um serviço de recepção terceirizado com limitações de custos, gerando uma baixa qualidade ou restrições na prestação dos serviços.

O uso de crachás de identificação ou adesivos se tornou uma prática comum, caracterizando apenas que a pessoa passou por algum cadastro. Contudo, são poucos aqueles em que se solicita documento com foto para conferência e se registra a saída. Esta prática serviu mais para poupar os funcionários de irem até a recepção acompanhar o visitante, além do mais, permite que esta pessoa estranha circule por ambientes os quais não informou na recepção.

Mann (2011), em um exercício prático apresentou-se ao segurança de uma empresa como visitante, contudo, posteriormente com uma atitude semelhante à dos funcionários que adentravam no mesmo horário passou pela recepcionista sem a devida identificação. "Era um risco aceitável, pois era uma hora movimentada do dia e ela provavelmente não perceberia. A maioria das pessoas que desempenha papéis repetitivos trabalha quase que exclusivamente no subconsciente e não percebe esse tipo de coisa." (MANN, 2011, p. 51)

4.5 FUNCIONÁRIOS NOVOS

Seguir todos os procedimentos de contratação e inclusão de um novo funcionário pode ser burocrático e demorado. Contudo, importante para a segurança da corporação. Algumas vezes, por urgência de algum setor ou gerência, que podem ter sidos persuadidos por uma falsa confiabilidade, se disponibiliza acessos antes da conclusão de todo o processo seletivo. Esta premência oferece uma excelente oportunidade para a atuação da

Engenharia Social. Peixoto entende que: "A checagem de informações é no mínimo necessária para qualquer corporação que priva a segurança de seus clientes como de si própria." (2006, p. 22)

Segundo Mann (2011, p. 48):

> Fingir ser um funcionário novo é um papel particularmente eficaz para um engenheiro social. Eles são novos, portanto, você não espera reconhece-los. Além disso, você esperaria que eles pedissem informações, e não particularmente questionassem alguma falta de conhecimento da maneira pela qual as coisas são em geral feitas [...]

A perspicácia de um engenheiro social o torna em um ingênuo funcionário novo que necessita se familiarizar com a rotina da instituição e de credenciais para acessar os sistemas. Tarefa que é normalmente realizada pelo suporte técnico de forma prestativa e podendo ser até pelo telefone interno.

4.6 TERMO DE POLÍTICA DE SEGURANÇA

A Revista REAVI (2012) publicou uma pesquisa com profissionais de tecnologia da informação (TI), realizada por estudantes da FATEC, objetivando a análise de riscos decorrentes de ataques de engenheiros sociais. Um dos profissionais entrevistados foi questionado se o mesmo assinou um contrato de política de segurança sobre ouso indevido de equipamentos da empresa. Declarando que: "Não assinei nada e não vi nada sobre isso".

O Termo de Ciência das Políticas de Segurança de uma corporação ou outro documento similar não deveria ser tratado como uma mera formalidade. Mediante um documento bem estruturado têm-se uma oportunidade de orientar e conscientizar os integrantes e colaboradores de uma instituição.

4.7 AS MESAS DOS FUNCIONÁRIOS

Segundo Maulais (2016), com o uso mais corriqueiro das mídias digitais esperava-se uma redução considerável no manuseio de impressos. A geração abrangida por esta mudança tecnológica ainda "sente" a necessidade de manusear os documentos de forma física, apesar das variadas ferramentas digitais já disponíveis.

Desta forma, informações relevantes contidas em documentos dispostos sobre as mesas continuam sendo uma vulnerabilidade para a segurança das informações. "É uma boa prática instituir o princípio de mesa limpa, isto é, o funcionário é instruído a deixar o seu local de trabalho sempre limpo e organizado, guardando os

documentos confidenciais tão logo não precise deles". (BUENO NETO, SOLONCA, 2007, apud MAULAIS, 2016).

Uma variante da técnica de leitura sobre os ombros pode ser aplicada nestes casos. Uma simples folha sobre a mesa pode municiar um engenheiro social de muitas informações.

4.8 FUNCIONÁRIOS INSATISFEITOS/DEMITIDOS

Danúbia e Jane (2008) relatam que, de acordo com uma pesquisa realizada nos Estados Unidos pelo Instituto Ponemon, seis em cada dez funcionários admitiram furtar dados da empresa ao deixar o emprego. As informações privilegiadas adquiridas de forma ilícita teriam sido usadas como benefício em um novo emprego, como subsídios na implementação de seu próprio empreendimento ou até mesmo por vingança.

Cássio Alves entende que um funcionário que se sente insatisfeito e desvalorizado pela empresa se torna uma vulnerabilidade em vários aspectos, inclusive da segurança da informação. Atualmente, ainda vivenciamos os "efeitos Snowden" como experiência mundial. "Todo o investimento em tecnologia, treinamentos e conscientização, pode ser jogado fora se a companhia não cuidar e valorizar seus funcionários." (PRESCOTT, 2007apud ALVES, 2010, p. 36)

De acordo com a Pesquisa Global de Segurança da Informação, divulgada pela PwC (2016, p. 26), os empregados foram responsáveis por 34% e os ex-empregados por 29% dos incidentes de segurança em 2015.

4.9 FUNCIONÁRIOS QUE TRABALHAM EM CASA

Segundo Mann (2011), assumir a identidade de pessoas que trabalham de casa pode ser uma manobra útil para enganar o escritório para que informações sejam repassadas. Uma ação direta sobre esta categoria de funcionários também pode ser explorada pela engenharia social devido ser um ambiente externo e consequentemente alheio a todos os protocolos de segurança da empresa.

4.10 LIXO

O lixo produzido por uma corporação pode se tornar uma excelente fonte de informações para a atuação de um engenheiro social. Talvez já se tenha uma preocupação com a destinação de relatórios com

informações sensíveis, mas qualquer impresso que possua algum dado sobre a rotina ou atividades realizadas pela empresa já serão úteis como subsídio para um futuro ataque mais elaborado.

A coleta do lixo pode ser realizada após o seu descarte nas lixeiras, através de uma observação da rotina. Outra forma de ação, se dá coletando o lixo de dentro da própria corporação, visando-se algum setor específico, tais como: o setor financeiro, o departamento de compras, a gerência e outros.

O reaproveitamento de folhas como rascunho é uma ação de sustentabilidade e de economia para a empresa. Contudo, antes de ser destinado como rascunho, necessita de uma atenção quanto ao seu conteúdo. Maulais (2016) classifica a análise do lixo como uma das técnicas mais empregadas pela Engenharia Social. Devido principalmente a baixa preocupação que as empresas têm com o descarte de seu lixo.

5 CONSIDERAÇÕES FINAIS

O objetivo geral desta pesquisa foi conhecer como os ataques diretos e pessoais da Engenharia Social se relacionam com a obtenção de informações de uma Corporação. Observou-se que mesmo com a sofisticação e implementação de inovações tecnológicas da informação, as instituições e seus integrantes, dos mais variáveis níveis, continuam vulneráveis. De tal modo que mais de 40% das falhas à Segurança da Informação não está associada à tecnologia (DARYUS, 2014; apud MAULAIS, 2016), e pouco se questiona sobre esta parcela.

Inicialmente no primeiro capítulo, foram abordadas as definições de Engenharia Social e suas formas de atuação. Para tanto, realizou-se uma pesquisa literária contemplando desde Mitnick (2003) até Maulais (2016), passando por outros autores não menos importantes. Constatou-se a existência de uma boa e variável literatura de especialistas, na qual suas ideias se apresentaram convergentes, sendo claro pautar tais entendimentos.

No segundo capítulo buscou-se definir um ataque direto e pessoal de um engenheiro social e caracterizar a atuação nesta forma, dando-se continuidade na coleta livros, artigos científicos e documentos de orientações de empresas de TI. Nesta forma mais específica de atuação da Engenharia Social, deparou-se com limitações na literatura mais atual, embora ser considerada uma das técnicas mais empregada para Maulais (2016). A maioria das publicações tem abordado os ataques da Engenharia Social na forma indireta, ou seja, aquelas associadas à tecnologia.

E finalizando, o terceiro capítulo objetivou relacionar vulnerabilidades de uma corporação a um ataque da engenharia social na forma direta e pessoal. Com a realização de uma ampla pesquisa literária, incluindo além dos já citados: revistas técnicas, monografias acadêmicas e experiências de especialistas. Pode-se compilar uma boa variedade de possibilidades de vulnerabilidades em setores ou funções de uma corporação que podem ser exploradas por um engenheiro social com a aplicação de variadas técnicas.

Considerando-se a revisão bibliográfica realizada, se observa que a Engenharia Social possui como característica essencial, a persuasão sobre o ser humano. Os engenheiros sociais se utilizam de habilidades

artísticas, científicas e técnicas direcionadas a explorar e manipular as fragilidades humanas, e não as tecnológicas, como os crackers (antigos hackers).

A forma direta e pessoal de atuação dos engenheiros sociais, apesar de se valerem de técnicas simples e aparentemente "manjadas", ainda são constantemente aplicadas e eficazes. Visualizando-se o crescimento em variedade e complexidade das ameaças tecnológicas que atingem as instituições, observou-se uma despreocupação e uma ignorância funcional referente esta forma de atuação. O que acaba propiciando maiores facilidades para o êxito silencioso do engenheiro social.

A última parte da pesquisa buscou disponibilizar uma lista de "dicas" que possa contribuir no aprimoramento dos Análises de Riscos e procedimentos de segurança de uma corporação. Pretendeu-se atender os anseios dos mais de 85% que consideram que o principal fator crítico para a segurança da informação está contido nos temas: Capacitação e Mudança de cultura organizacional (DARYUS, 2014, p. 17).

Portanto, ao longo desta pesquisa os objetivos específicos foram alcançados, utilizando uma abordagem qualitativa que forneceu material satisfatório para a explanação da relevância desta particular forma da atuação da Engenharia Social sobre as corporações. Tal resultado foi obtido devido à variedade de profissionais e acadêmicos preocupados com o tema, somando-se um total de dezenove publicações e trabalhos consultados. Porém, observou-se uma escassa literatura nacional disponível, sendo consultada apenas cinco obras nacionais.

É importante que mais pesquisas qualitativas sejam executadas e disponibilizadas na literatura a fim de especificar o considerável percentual de falhas da Segurança da Informação que não estão associadas à tecnologia.

REFERÊNCIAS

ALVES, Cássio Bastos. Segurança da informação vs. Engenharia social - como se proteger para não ser mais uma vítima. 2010. 63 f. Artigo (Bacharel em Sistemas da Informação) Centro Universitário do Distrito Federal – UDF, Brasília. Disponível em: < https://s3.us-east-2.amazonaws.com/administradores-website /_assets/modules/academicos/academico_3641.pdf>. Acesso em: 20 fev. 2017.

ANDRADE, Danúbia; CUNHA, Jane de Souza. Engenharia Social e a Vulnerabilidade Humana. 2008. (Tecnólogo em Redes de Computadores) Faculdade Estácio de Sá de Goiás – FESGO, Goiânia. Disponível em: <www.tatudoaki.com.br/download_trab/419>. Acessado em: 22 set. 2017.

BRASIL. Código Penal Brasileiro. Decreto-Lei Nr. 2.848, de 7 de dezembro de 1940. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848 compilado.htm>. Acesso em 06 jan. 2017.

BUENO NETO, Abílio; SOLONCA, Davi. Auditoria de sistemas informatizados. 3. ed. Palhoça: Unisul Virtual, 2007 apud MAULAIS, Claudio Nunes dos Santos, 2016.

CARRO, Rodrigo. Cisco reforça aposta em segurança. maio 2014. Disponível em: <http://brasileconomico.ig.com.br/negocios/2014-05-29/cisco-reforca-aposta-em-seguranca.html>. Acesso em: 18 jan. 2018.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; DA SILVA, Roberto apud CUSTÓDIO, Nayara Fernanda Silva, 2012. Metodologia Científica. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

DARYUS Consultoria, Educação e Tecnologias. Pesquisa_ISM. Disponível em: <http://conteudo.daryus.com.br/pesquisa-nacional-de-seguranca-da-informacao -2014>. Acesso em: 15 set.de 2017.

FRISCH, A. Essential System Administration, 2a. ed. Sebastopol - CA: O'Reilly. 1995.

GARTNER, INC. Protect Against Social Engineering Attacks in Gartner's Information Security Strategies Research, Volume 1, Issue 1, February 2002, apud BALDIM; Natália Pimenta. Engenharia Social e Segurança da Informação no Ambiente Corporativo: uma análise focada nos profissionais de Secretariado Executivo, (Secretariado Executivo Trilíngue) – Universidade Federal de Viçosa, 2007.

GOLDENBERG, 1997, p. 34 apud GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo (Organizadoras) UFRGS – Métodos de Pesquisa, 2009.

MANN, Ian. Engenharia Social. Traduzido por Editora Longarina – São Paulo: Blucher, 2011.

MARCELO, Antonio; PEREIRA, Marcos. A Arte de Hackear Pessoas. Rio de Janeiro: Brasport, 2005 apud ALVES, Cássio Bastos. Segurança Da Informação Vs. Engenharia Social - Como Se Proteger Para Não Ser Mais Uma Vítima. Brasília, 2010.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria apud CUSTÓDIO, Nayara Fernanda Silva, 2012. Fundamentos de metodologia científica. 7. ed. São Paulo: Atlas, 2010.

MAULAIS, Claudio Nunes dos Santos. Engenharia social: técnicas e estratégias de defesa em ambientes virtuais vulneráveis. 2016. Projeto de pesquisa (Mestrado em Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, Belo Horizonte. Disponível em: <http://www.fumec.br/revistas/sigc/article/viewFile/ 3733/2031>. Acesso em: 20 ago. 2017.

MCCARTHY; Mary Pat; Campbell, Stuart. Brownstein, Rob. Transformação na Segurança Eletrônica. Tradutor:

PASCHOA, C. R. São Paulo, Pearson Education do Brasil, 2003 apud ANDRADE, Danúbia; CUNHA, Jane de Souza. Engenharia Social e a Vulnerabilidade Humana. Faculdade Estácio de Sá de Goiás (FESGO) - Goiânia, 2008.

MICROSOFT CORPORATION. Como proteger as pessoas de dentro da empresa contra ameaças de engenharia social. Publicado em: 18 de agosto de 2006. Disponível em: <https://technet.microsoft.com/pt-br/pt%C2%ADbr/library/cc875841 (d=printer).aspx>. Acessado em 16 jan. 2017.

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

PARDINI, D.J.A apud MAULAIS, Cláudio N.S. Transformação cultural no processo de aquisição de empresas relacionadas do setor siderúrgico. Tese de Doutorado em Administração de Empresas - UFMG/CEPEAD, Belo Horizonte. 2004.

PEIXOTO, Mário César Pintaudi. Engenharia social e segurança da informação na gestão corporativa. Rio de Janeiro: Brasport, 2006.

PRESCOTT, Roberta. Fator humano: um dos pilares da segurança da informação. 2007 apud ALVES, Cássio Bastos. Segurança da informação Vs. Engenharia social - Como se proteger para não ser mais uma vítima. Brasília, 2010.

PwC, Inovando e Transformando em segurança cibernética. Pricewaterhouse Coopers Brasil Ltda. 2016. Disponível em: <https://www.pwc.com.br/pt/publicacoes /servicos/assets/consultoria-negocios/2016/tl-gsiss16-pt.pdf>. Acessado em 10 nov. 2017.

ROSA, Adriano Carlos; SILVA, Bruno Donizete da; SILVA, Pedro Lemes da. Análise de redes sociais aplicada à engenharia Social. In: Anais do I SINGEP. São Paulo, SP, Brasil, 2012, apud MAULAIS, Claudio Nunes dos Santos, 2016.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva da segurança da informação. 9ª reimpressão. Rio de Janeiro: Elsevier, 2003, apud BALDIM; Natália Pimenta, 2007.

SILVA, Clayton S. et al. Engenharia Social: O elo mais frágil da segurança nas empresas. **Revista Eletrônica do Alto Vale do Itajaí**. N° 02. Dezembro 2012. Disponível em: < http://www.revistas.udesc.br/index.php/reavi/issue/view/260>. Acesso em: 20 set. 2017.

SILVA, Abner Oliveira e. Engenharia social: o fator humano na segurança da informação. Coleção Meira Mattos: Revista Das Ciências Militares, CMM/ PADECEME 3° quadrimestre de 2010. Disponível em: <http://portal.eceme. ensino.eb.br/meiramattos/index.php/RMM/issue/view/2/showToc>. Acessado em 16 jan. 2017.

SILVA FILHO, Antônio Mendes da. Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações in Revista Espaço Acadêmico n° 43 – dezembro 2004.

SIQUEIRA, Marcelo Costa. Gestão estratégica da informação. Rio de Janeiro: Brasport, 2005.

VASCONCELOS, Eduardo. Engenharia social: por que se importar? Maio. 2017. Disponível em: <https://www.linkedin.com/pulse/engenharia-social-por-que-se-importar-eduardo-vasconcelos/>. Acessado em 19 jan. 2017.

TATSCH JUNIOR, Evaldo, 2009 apud SILVA, Abner de Oliveira e. Engenharia social: o fator humano na segurança da informação. Coleção Meira Mattos: Revista Das Ciências Militares, CMM/PADECEME 3° quadrimestre de 2010. Disponível em: <http://portal.eceme.ensino.eb.br/meiramattos/index.php/RMM/issue/view/2/showToc>. Acessado em 16 jan. 2017.