ENGENHARIA SOCIAL: SEGURANÇA DA INFORMAÇÃO APLICADA À GESTÃO DE PESSOAS - ESTUDO DE CASO

Leandro de Deus PEREIRA
Centro de Ensino Superior de Juiz de Fora, Juiz de Fora, MG
Daves Márcio Silva MARTINS

Resumo: A Informação é considerada como o maior bem de uma organização atualmente, por isso há uma necessidade crescente de protegê-la. O presente trabalho realiza um estudo de caso com o objetivo de investigar o nível de preparo das organizações para lidar com o uso da engenharia social no processo de obtenção de informações. Para a realização do estudo, foi aplicado um questionário a profissionais de diferentes instituições. Como resultado é possível notar a ocorrência de elevado percentual de usuários explorados pela engenharia social, gerando portanto fragilidades no processo de segurança da informação. Em conclusão, é possível perceber ausência ou falha na política de segurança da informação das instituições. Sugere-se portanto, que trabalhos de conscientização dos usuários da tecnologia da informação devam receber maior atenção para melhor proteger as informações.

Palavras-chave: Segurança da Informação; Engenharia Social; *Phishing*; Prevenção de ataques.

1 INTRODUÇÃO

A Informação é considerada como um dos maiores patrimônios de uma organização nos dias de hoje, por isso há uma necessidade crescente de protegê-la (MOREIRA, 2012). Entretanto, seus esforços para promover a proteção das informações têm sido direcionados aos recursos físicos e lógicos, tornando-as, aparentemente, cada vez menos vulneráveis aos atacantes (SILVA FILHO, 2013).

Outro importante ponto a ser protegido consiste no fator humano, o qual tem sido deixado em segundo plano quando deveria receber mais atenção, pois é ele quem opera os sistemas e está suscetível a erros. Os atacantes, cientes dessa fraqueza, exploram cada vez mais o fator humano através da engenharia social (ALVES, 2010).

Engenharia Social é um termo empregado na qualificação dos tipos de intrusão não técnica, com ênfase na interação humana (SILVA FILHO, 2004).

Diante da realidade que aponta o fator humano como o componente mais susceptível à transmissão indevida das informações das empresas, faz-se necessário conhecer melhor os hábitos dos funcionários das empresas a fim de aumentar a proteção das informações.

Dessa forma, o presente trabalho realiza um estudo de caso com o objetivo de investigar o nível de preparo das organizações para lidar com o uso da engenharia social no processo de obtenção de informações.

2 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO E ENGENHARIA SOCIAL

2.1 SEGURANÇA DA INFORMAÇÃO

Intensamente conectado pelas redes de telecomunicações, o mundo globalizado considera como de vital importância, a informação dentro de uma organização moderna. Para manterem-se competitivas no mercado, essas organizações devem gerenciar e proteger suas informações (MOREIRA, 2012).

Segundo Silva Junior (2009), no começo da informática a questão de segurança da informação era muito mais simples, pois os ativos digitais de uma organização ficavam em um lugar chamado Central de Processamento de Dados (CPD), mas com a rápida evolução da TIC, a questão ficou bem mais complexa. Hoje podemos encontrar informações das empresas circulando em *notebooks*, fitas de *backup*, CDs, *pendrives*, *smartphones*, e-mails, etc. Para Moreira (2012), esta circunstância transformou estes ativos em grande atrativo para ladrões. Além disso, outras circunstâncias como desastres naturais, problemas elétricos, uso incorreto dos sistemas, engenharia social, entre outros, colocam em risco os sistemas de informação.

Desta forma pode-se afirmar que não existe informação totalmente segura, é necessário buscar as vulnerabilidades do sistema de informação, avaliar os riscos e impactos para providenciar medidas que intensifiquem a segurança da informação e prover seus princípios elementares que são: integridade, confidencialidade e disponibilidade (PEIXOTO, 2012).

A NBR ISO/IEC 27002 é conhecida como uma norma para os códigos de práticas para gestão de segurança da informação. Essa norma é mundialmente aceita, ela faz referência aos requisitos que devem ser implementados nas organizações (PEIXOTO, 2012).

As pessoas são os elementos mais frágeis dos sistemas de informação, por isso as soluções técnicas não são suficientes para garantir sua segurança, assim, os conceitos referentes à segurança da informação devem ser compreendidos e

seguidos por todos os funcionários de uma instituição, em todos os níveis hierárquicos (MOREIRA, 2012).

2.1.1 ASPECTOS GERAIS DA SEGURANÇA DA INFORMAÇÃO

Cerutti (2012) afirma que o programa de segurança da informação deve iniciar pelas pessoas, pois segurança não envolve apenas tecnologia.

Pode-se observar na Figura 1, um diagrama que mostra o inter-relacionamento entre os componentes envolvidos nos planejamentos relacionados com segurança da informação.

FIGURA 1: Diagrama de inter-relacionamento entre componentes da segurança da informação.

Fonte: CERUTTI(2012)

Pessoas: São os elementos mais importantes na gestão da segurança, pois são elas que executam e dão suporte aos processos de uma organização. Deve se tratar com as pessoas os assuntos relacionados a esta área e estabelecer seus papéis e responsabilidades na organização. Processos: São os elementos que se bem definidos, tornam a segurança da informação uma responsabilidade de todos e não apenas da equipe de segurança. Essa gestão determina, por meio de diretrizes, as maneiras corretas de se agir nos processos da organização para que a segurança seja o mínimo afetada. Ferramentas: São os recursos físicos e lógicos da segurança, utilizados para dar suporte aos processos na organização. Tem como objetivo facilitar a aplicação das políticas de segurança da informação. Agregam várias funcionalidades, começando pela identificação dos usuários, defesa contra ameaças, criptografia dos dados e gestão da segurança (CERUTTI, 2012).

2.2 O QUE É ENGENHARIA SOCIAL

A prática da engenharia social é oriunda dos tempos mais remotos. Somente o termo é novo e ficou mais conhecido na década de 1990 com o hacker Kevin Mitnick (MARTINS, 2008).

Segundo Silva Filho (2004), engenharia social, na área de sistemas de informação, é um termo empregado na qualificação dos tipos de intrusão não técnica, que enfatiza a interação humana, envolvendo com frequência a habilidade de enganar pessoas, com o objetivo de violar procedimentos de segurança. O aspecto mais relevante na engenharia social envolve a inaptidão das pessoas em manterem-se atualizadas com as questões que envolvem a tecnologia da informação, que na maioria das vezes não tem consciência do valor das informações que possuem e, por isso, não se preocupam em protegê-las.

2.2.1 ENTENDENDO A ENGENHARIA SOCIAL

Ao contrário do que muitos pensam, engenharia social não se trata de um curso, mas sim, de técnicas. O engenheiro social nada mais é do que uma pessoa que acha mais fácil explorar a natureza humana do que buscar falhas técnicas em sistemas de informação, geralmente com a intenção de instalar softwares maliciosos ou induzi-lo a entregar suas senhas ou demais informações confidenciais, de natureza pessoal ou financeira, e que pode usar esse conhecimento também de forma benéfica, com o objetivo de encontrar falhas em um sistema de informação para aperfeiçoá-lo (MICROSOFT, 2014).

Sendo assim a engenharia social pode ser usada para diversos fins, podendo agredir ou não os valores morais. Um engenheiro social pode usar seus conhecimentos e táticas pessoais para buscar falhas e violar um sistema de segurança da informação de uma pessoa física ou jurídica a fim de obter informação de forma desonesta, objetivando lucro pessoal ou empresarial, enquanto outro pode usar das mesmas ferramentas para aperfeiçoar, corrigir e proteger o sistema de segurança da informação.

Para Braga (2010), a engenharia social pode parecer algo tolo e que só tem a capacidade de afetar o usuário leigo, mas na verdade é uma das maiores ameaças à segurança da informação na atualidade, é uma poderosa forma de se invadir os sistemas mais seguros. Possivelmente o fator humano jamais será removido dos

sistemas computacionais, por isso sempre existira a possibilidade de um ataque desse tipo. Quando a vítima descarta uma ameaça desse tipo, ela se torna ainda mais vulnerável, por isso, quem preza pela segurança da informação jamais deve ignorar esse tipo de ameaça.

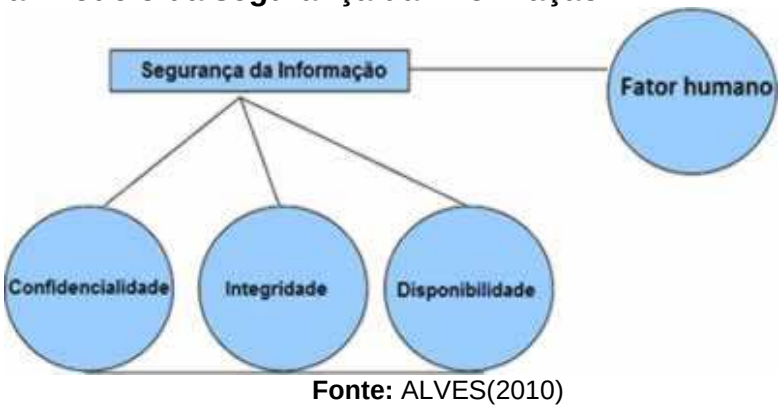
2.3 O FATOR HUMANO E SUAS VULNERABILIDADES

Segundo Braga (2010), na prevenção de um ataque à segurança da informação, geralmente se pensa logo na correção de falhas computacionais que podem levar ao sucesso destes ataques. Cercam-se os sistemas por *firewalls*, instalam-se antivírus e *anti-spywares* para detectar e remover programas maliciosos, atualizam-se sempre todos os programas na esperança de corrigir as suas falhas. Porém, por mais critérios que existam na política de segurança de um sistema, ele pode ser comprometido por seus usuários.

Para Braga (2010) o erro humano é considerado uma segunda rota de invasão para um sistema. Ele define o erro humano como sendo todo comportamento inseguro, seja ele contínuo ou fruto de um momento de distração, que pode ser usado por um engenheiro social mal intencionado para que este consiga comprometer o sistema. Braga afirma ainda que o grande problema com o erro humano é que ele não pode ser completamente corrigido, mas apenas minimizado, afinal nenhuma pessoa é perfeita e nenhum treinamento pode mudar isso.

O fator humano é o fator de desequilíbrio que sempre existirá em uma organização. Faz-se necessário a inclusão desse fator como sendo um elemento base da segurança da informação, o que está sendo discutido, por ainda não ser considerado no modelo atual, como mostrado Figura 2 (ALVES, 2010).

FIGURA 2: Atual modelo da segurança da informação



Fonte: ALVES(2010)

Segundo Alves (2010), uma das maiores causas de ataques a sistemas computacionais dá-se através do fator humano.

O ser humano é o elemento mais vulnerável em qualquer sistema, independente do hardware, software e plataforma utilizada, pelo fato do ser humano possuir traços psicológicos e comportamentais tornando-o susceptível a ataques de engenharia social. Dentre essas características, pode-se destacar (SILVA FILHO, 2004): Vontade de ser útil; Busca por novas amizades; Propagação de responsabilidade; Persuasão.

Segundo Nassaro (2012), as organizações devem estar atentas aos funcionários descontentes, que por algum motivo, podem usar as informações confidenciais da organização que o mesmo tem acesso para prejudicar a mesma.

3 MEIOS E TÉCNICAS DE ATAQUES DE ENGENHARIA SOCIAL

Existem vários meios e para cada meio, várias técnicas utilizadas em situações diversas, sempre explorando alguma das fraquezas citadas de uma pessoa ou de um grupo de pessoas. A maioria delas consiste em obter informações privilegiadas enganando usuários de determinado sistema com persuasão, identificação falsa, adquirindo carisma e confiança da vítima. Os ataques de engenharia social podem ter dois aspectos diferentes: o físico, como local de trabalho, por telefone, no lixo ou mesmo on-line, e o psicológico, que se refere à maneira como o ataque é executado, tal como persuasão.

3.1 MEIOS MAIS UTILIZADOS NA ENGENHARIA SOCIAL

Os meios mais utilizados na engenharia social segundo Alves (2010) e Nassaro (2012) são: Telefone convencional ou voz sobre IP (*VolP*): O engenheiro social usa suas técnica e habilidades passando-se por alguém para ludibriar a vítima; Internet: Coletar informações sensíveis dos usuários como, por exemplo, *login* e senha ao serem digitados; Intranet: Tem por objetivo acessar remotamente algum microcomputador da rede com o objetivo de se passar por alguém; E-mail: Enviar e-mails falsos para induzir a vítima a clicar em *links* que instalarão *softwares* maliciosos ou redirecionarão para páginas falsas que capturam dados digitados; Pessoalmente: constitui uma visita *in loco* por parte do transgressor para

levantamento de informações ou para execução de ações. Talvez seja o menos utilizado, pois o que atrai um engenheiro social é a obscuridade que essa técnica fornece. Mas, apesar do risco, às vezes essa é a única alternativa que resta aos criminosos; Correio convencional: Envia correspondências ou cartas falsas para as vítimas. É um método considerado nada atual, mas é muito utilizado para enganar pessoas mais antigas ou idosas; *Spyware*: É um *software* espião que monitora o microcomputador sem que a vítima perceba; Redes *P2P* (*Peer-to-Peer*): Essa é uma tecnologia que permite o compartilhamento de arquivos entre diversos computadores. O atacante usa essa tecnologia para espalhar *softwares* maliciosos, além de oferecer ajuda para suas vítimas a fim de trapaceá-las; Redes sociais: Os sites de relacionamento são cada vez mais utilizados pelos usuários. O que muitos deles talvez não saibam é que esses sites deixam um rastro das informações de maneira que pessoas mal intencionadas possam se passar por outras pessoas, camuflando assim sua real identidade. Isso contribui bastante para o sucesso de um ataque de engenharia social.

3.2 TÉCNICAS DE ENGENHARIA SOCIAL

As técnicas e os métodos mais utilizados na engenharia social, segundo Alves (2010) são:

- Pesquisa: Essa tática concerne no colhimento de materiais com a finalidade de descobrir quem são as pessoas que guardam as informações desejadas. O próximo passo será procurar meios para absorver as informações desejadas dessas pessoas.
- Personificação e impostura: A personificação se baseia na criação de um personagem. Um exemplo clássico é aquele em que o engenheiro social faz uma ligação passando-se por alguém da área de informática da empresa e diz precisar da senha da pessoa, ou se passar por um assistente da presidência ou gerencia para pedir informações em nome do seu chefe. Muitos engenheiros sociais chegam a estudar padrões de fala e o tipo de linguagem utilizada por suas vítimas, pois cada organização possui suas próprias linguagem e expressões. Isso acontece porque ao conversar com alguém utilizando a mesma linguagem, se torna mais fácil persuadi-lo, pois a vítima se sente mais segura. Em grandes empresas é difícil conhecer todos os funcionários e devido a isso, normalmente a vítima acaba cedendo.

- Divisão de responsabilidades: A técnica da divisão de responsabilidades também é bem comum e se resume em convencer os funcionários a compartilharem as senhas com o objetivo de dividirem determinadas tarefas ou responsabilidades.
- *Spoofing*: Uma nova técnica utilizada é o chamado *Spoofing* de identificador de chamadas, que tem o objetivo de fraudar o número de telefone, fazendo com que o número exibido pelo identificador de chamadas seja aquele desejado pelo fraudador (JUSTASKGEMALTO, 2014).
- E-mails falsos: Essa técnica é uma das mais comuns aplicadas pelos engenheiros sociais para conseguirem dados alheios como, por exemplo, senhas, contas bancárias, cartões de crédito, etc. Normalmente esses e-mails falsos abordam assuntos que estão em alta na mídia, atualizações de segurança, recuperação de dados bancários, promoções, premiações ou qualquer outro assunto que venha despertar a curiosidade da vítima para que ela seja persuadida a clicar em *links* que instalarão *softwares* maliciosos ou direcionarão para páginas falsas, que capturarão os dados da vítima ao serem digitados.
- *Phishing*: É um tipo de golpe eletrônico cujo objetivo é o furto de dados pessoais. Esta técnica merece mais atenção e será vista mais adiante.
- Engenharia social inversa: A engenharia social inversa é uma técnica mais avançada e que exige muito mais preparação e pesquisa. Nessa técnica os papéis se invertem. O atacante finge ser uma autoridade, de maneira que os funcionários passarão a pedir informação para ele, até chegar um ponto que o criminoso extrairá informações valiosas sem que ninguém desconfie.
- *Footprint*: Essa técnica tem por objetivo maior, descobrir informações a respeito de algumas tecnologias usadas pela empresa, referentes principalmente ao acesso remoto, internet e intranet. Essa técnica utiliza-se de softwares especiais para coletar as informações desejadas e é normalmente utilizada quando o invasor não consegue absorver as informações desejadas através de outras técnicas de persuasão devido à falta de conhecimento por parte das vítimas a respeito do assunto desejado pelo invasor.
- Vasculhar o lixo: Vasculhar o lixo da empresa é um dos grandes métodos usados por esses criminosos para conseguirem acessar informações sensíveis, pois muitas empresas não se preocupam com o destino do seu lixo ou sequer utilizam máquinas fragmentadoras ou trituradoras de papel para que os

diversos documentos sigilosos não sejam recuperados por pessoas mal intencionadas.

- Olhar pessoas digitando: Essa técnica tem por objetivo descobrir as senhas das pessoas enquanto elas digitam no teclado.
- Programação neurolinguística: Essa técnica baseia-se em imitar o jeito de ser da vítima como, por exemplo, sua maneira de falar, se expressar, gestos e entre outros, por um determinado tempo para assim confundi-la, de maneira a formar certa intimidade, deixando a vítima pensar que está no comando da situação. Até que a partir de certo momento, o engenheiro social passa a comandar o diálogo sem que a vítima sequer perceba, capturando assim as informações desejadas.

3.2.1 PHISHING

Segundo Weinberg (2013), 95% de todos os ataques contra redes corporativas são resultados de ataques bem sucedidos de *phishing*.

Phishing consiste do envio de mensagens falsas para a vítima, buscando obter, sem o conhecimento desta, informações sigilosas. Seu funcionamento baseia-se na exploração de um vínculo de confiança entre a vítima e por quem o atacante está se passando (Braga, 2010).

Furtado (2012) define *phishing* como sendo um tipo de golpe eletrônico cujo objetivo é furto de dados pessoais. Esses golpes eletrônicos podem ocorrer de diversas maneiras. As mais comuns são:

- *Phishing* por e-mail: E-mails com mensagens de depósitos ou de prêmios são comuns. Geralmente esses e-mails contam com um *link* que leva a uma página sem sentido para o usuário. Este tipo de golpe instala programas chamados de cavalos de tróia ou *trojans* no computador do usuário. Uma vez instalado, esses programas monitoram praticamente qualquer atividade e capta dados importantes do usuário.
- *iPhishing*: É uma variação do tradicional *phishing*. Esta variante explora deficiências de segurança em dispositivos modernos. Sua manifestação mais comum é o envenenamento do *Domain Name System (DNS*). Esse procedimento limita o usuário a acessar apenas os sites programados.
- *Phishing* por mensageiros instantâneos: A contaminação acontece através de um *link* que, se clicado, instala um programa malicioso que captura os dados do usuário. O maior problema são os computadores de seus contatos que,

caso infectados, enviam os *links* maliciosos para contaminar toda sua lista de contatos.

- *Phishing* por sites de relacionamentos: Atualmente é um dos meios preferidos dos estelionatários virtuais. Isso ocorre pelo número de compartilhamentos realizados nestas redes, e pelo nível alto de confiança que os usuários depositam nestes ambientes.

4 FORMAS DE PREVENÇÃO AOS ATAQUES

A prevenção não é uma tarefa fácil. As empresas podem adquirir os mais avançados equipamentos tecnológicos, e a maioria delas investem grandes quantias em sistemas e novas tecnologias, mas essas empresas devem se conscientizar e direcionar recursos financeiros para combater a engenharia social, que é uma ameaça real e pode ser bem mais perigosa que outras ameaças.

Os seres humanos costumam modificar seus comportamentos em situações de risco, e suas decisões são baseadas em confiança. A engenharia social se aproveita dessas brechas e da falta de consciência com relação à segurança. Costa (2013), afirma que a melhor arma para combater a engenharia social é a informação. Se os colaboradores de uma empresa não estiverem bem treinados e bem informados dos golpes envolvendo engenharia social, de nada adiantará os demais investimentos em meios tecnológicos voltados para segurança. Para minimizar essas falhas, a gestão de uma empresa deve considerar altamente relevante as suas informações e assim criar uma cultura corporativa que tenha como prioridade capacitar seus colaboradores a partir da admissão, através de programas de treinamento.

Os planos de segurança de uma organização devem prever a atuação de seus agentes responsáveis na dedicação de tempo razoável aos demais colaboradores com o intuito de o familiarizarem com as políticas e procedimentos de segurança.

4.1 POLÍTICA E PROCEDIMENTOS DE SEGURANÇA

As informações importantes de uma organização estão expostas a diversos tipos de ataques, sejam eles através de meios lógicos, físicos ou humanos. E como dito anteriormente, na maioria das empresas o fator humano é deixado em segundo

plano, e é justamente neste ponto que entra o engenheiro social, atuando para ter acesso a essas informações confidenciais.

Para amenizar estes riscos, é necessário criar políticas de segurança centralizadas e bem divulgadas, para que seus colaboradores possam ter conhecimento sobre segurança da informação, o que é uma informação confidencial e o que não é confidencial, o que fazer em situações de risco e a quem reportar (Costa, 2013). As *intranets* podem ser um bom recurso para essa divulgação, assim como boletins periódicos *on-line*, lembretes no correio eletrônico e requisitos de mudança de senha. Para que os funcionários não se tornarem complacentes e relaxarem na segurança, a insistência é importante.

Poper e colaborador (2002), lista uma série de riscos, táticas e estratégias de combate a serem utilizadas na elaboração de uma política de segurança da informação

4.1.1 PROTEÇÃO CONTRA ATAQUES DE PHISHING

Enquanto alguns ataques de *phishing* envolvem o envio de mensagens em massa, outros podem parecer que foram enviados pelo departamento de TI da empresa, por outros departamentos, ou até mesmo por alguém conhecido.

Para se proteger desse perigo, as seguintes recomendações podem ser seguidas (Weinberg, 2013):

- Ler a URL do site de trás para frente. Comece pelo fim. O endereço pode muito bem começar com "www.seubanco.com.br", mas quando terminar com vários caracteres sem sentido, pode desconfiar;
- Não cair no que está sendo chamado de "*phishing* de mão dupla", em que você pode responder ao *e-mail* com uma pergunta, "Você é realmente meu amigo Jim?". Cibercriminosos são espertos o suficiente para esperar um pouco, mostrar que a resposta não é automatizada, e então responder com: "Sim, sou eu, Jim". É claro que não é ele;
- Nunca abrir um arquivo em PDF de alguém que você não conhece, afinal *crackers* podem se aproveitar para esconder seus arquivos maliciosos e executáveis dentro desses arquivos aparentemente inofensivos;
- Jamais fornecer senha ou informações pessoais/confidenciais em resposta a uma consulta não-solicitada;

- Profissionais de segurança de TI devem considerar treinamentos que visem especificamente *spear phishing*;

4.1.2 PLANO DE TREINAMENTO E CONSCIENTIZAÇÃO

Como o foco deste trabalho é a engenharia social, seu impacto e como combatê-la, faz-se necessário incluir no plano de treinamento dos colaboradores, meios de controle dos riscos inerentes aos fatores humanos. Alves (2010), lista os seguintes meios de controle que não devem faltar no plano de treinamento dos colaboradores: Seminários de sensibilização; Cursos de capacitação; Campanhas de divulgação da política de segurança; Crachás de identificação; Procedimentos específicos para demissão e admissão de funcionários; Termo de responsabilidade; Termo de confiabilidade; Software de auditoria de acessos e Software de monitoramento e filtragem de conteúdo.

As práticas supracitadas não cessarão, mas ajudarão a minimizar a possibilidade da organização se tornar mais uma vítima da engenharia social.

5 ESTUDO DE CASO

Para a realização do estudo de caso, foi elaborado um questionário composto por 41 perguntas (ANEXO 1). A construção das perguntas foi baseada em estudo anterior desenvolvido por Baldim (2007).

O questionário foi aplicado a 58 profissionais de empresas de diversos portes e diversos seguimentos de mercado, que, por questões de segurança e privacidade, tiveram preservados seus nomes, e o de suas empresas, bem como outras informações corporativas.

A aplicação do questionário foi realizada através da utilização de uma plataforma eletrônica SurveyMonkey.com (https://pt.surveymonkey.com/).

Afim de evitar equívocos de percentual no cruzamento de informações, os questionados que deixaram perguntas em branco não fizeram parte da análise.

5.3 RESULTADOS E DISCUSSÃO

Os resultados permitiram identificar vulnerabilidades no processo de segurança da informação das empresas a partir do fator humano.

A análise dos resultados da pesquisa, composta por 58 questionados que responderam integralmente o questionário ofereceu as seguintes informações.

Dos questionados (n = 58), 81,03% (n = 47) possuem curso de pós-graduação ou nível superior e 82,76% (n = 48) são profissionais de TI. Adicionalmente, 98,28% (n = 57) dos questionados afirmaram saber o que é segurança da informação e 72,41% (n = 42) afirmaram conhecer o tema engenharia social.

Embora o conhecimento sobre segurança da informação seja unânime entre os profissionais de TI, 15,51% (n = 7) responderam não conhecer o tema engenharia social. O número de profissionais que desconhece o assunto abordado é reduzido em relação ao total de profissionais (n=48), uma vez que o desempenho da profissão em TI não é regulamentada, não exigindo uma formação específica, o que conseqüentemente pode promover a falta de conhecimento a cerca do tema engenharia social.Tal realidade sugere que o assunto engenharia social se encontra bem conhecido, entretanto, uma maior divulgação do mesmo através de abordagens promovidas por profissionais em TI mais capacitados, pode aumentar a possibilidade de se proteger melhor as informações.

A engenharia social se utiliza de diferentes vias para obter as informações e segundo Weinberg (2013), as técnicas de *phishing* representam 95% dos ataques bem sucedidos contra redes corporativas.

A investigação sobre a possibilidade de ser enganado pela técnica de *phishing* no presente estudo, se deu através da aplicação da pergunta " Se você recebesse um email informando uma premiação e solicitando clicar sobre um link para maiores informações, o que faria?" (TABELA 1).

TABELA 1: Reação aos e-mails duvidosos

Se você recebesse um e-mail informando sobre uma premiação e solicitando clicar sobre um link para maiores informações, o que faria?

OPÇÕES DE RESPOSTA	PROPORÇÃO (%)	NÚMERO DE QUESTIONADOS
Clicaria sobre o link	1,72	1
Enviaria para análise do setor de TI	3,45	2
Apontaria o mouse para o link sem clicar	39,66	23
Apagaria o e-mail imediatamente	55,17	32
TOTAL	100%	58

O valor de n = 1 representa um baixo percentual em relação ao total da amostra, sugerindo que os questionados encontram-se atentos para as tentativas de

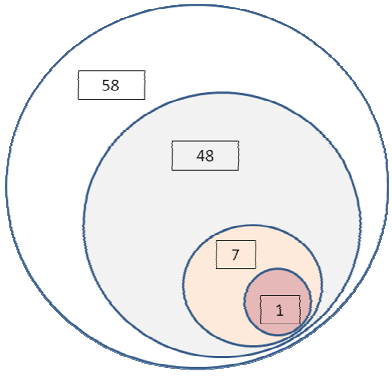
ataque de *phishing* por email. Entretanto, cabe ressaltar que o cruzamento dos dados relativos à presente pergunta e às perguntas " Em que área você trabalha?" e " Você sabe o que é Engenharia Social?" revelou a ocorrência de um profissional de TI, que não conhecia engenharia social e que clicaria sobre o link relativo à pergunta que investiga o preparo dos usuários para tentativas de *phishing*.

Inicialmente foram detectados os profissionais de TI que desconhecem o tema engenharia social a partir do total de questionados, o que ofereceu um número de 7 indivíduos. Destes, 57,12% (n = 4) afirmam já ter recebido e-mail fraudulento (Tentativa de *phishing*) e 14,28% (n = 1) disseram que se recebessem um e-mail informando sobre uma premiação e solicitando clicar sobre um *link* para maiores informações, clicariam sobre o *link* (*phishing*).

Dessa forma, um valor considerado pequeno dentro da amostra, sugere que a falta de informação sobre engenharia social, que ocorre mesmo entre os profissionais de TI, pode favorecer a perda de informações. Para melhor entendimento da análise descrita, foi elaborada a figura 3:

Afim de conhecer o nível de percepção dos entrevistados sobre a condição de segurança da informação das organizações em que trabalham, foi realizada uma correlação dos dados obtidos a partir da pergunta " Você acha que seria difícil para pessoas externas conseguirem informações importantes da empresa?". Os dados correlacionados foram os profissionais de TI que desconhecem o tema engenharia social (n = 7) e os que responderam conhecer o tema engenharia social (n = 41).

FIGURA 3: Relação de questionados sujeitos ao ataque de *phishing* por email.



Nota: Círculo maior externo representa o total da amostra (n=58); círculo maior interno representa sub-amostra do total, composta por questionados profissionais em TI (n=48); círculo médio interno é composto por questionados que responderam não conhecer engenharia social (n = 7); círculo pequeno interno constituído por questionados que responderam "clicaria sobre o link" (n = 1) para a pergunta "Se você recebesse um email informando uma premiação e solicitando clicar sobre um link para maiores informações, o que faria?".

A partir desses, identificou-se um valor de 71,40% (n = 5) de indivíduos que consideram que as informações importantes da empresa estão seguras e 46,34% (n = 19) dos indivíduos que afirmam conhecer engenharia social consideram que as informações importantes da empresa estão seguras. Diante desses dados é possível sugerir que haja uma falsa percepção de segurança da informação por desconhecimento do tema engenharia social, fato que pode ser evidenciado pela observação dos percentuais de um menor percentual (46,34%) obtido a partir da investigação sobre o mesmo tema com os profissionais de TI que conhecem o assunto engenharia social, quando comparado aos que o desconhecem (71,40%). Os profissionais conhecedores da engenharia social e conscientes de possíveis falhas de segurança da informação (53,66%; n = 22) estão possivelmente mais capacitados não só para reconhecer as vulnerabilidades, mas também para auxiliar no processo de implantação de uma efetiva política de segurança da informação nas organizações.

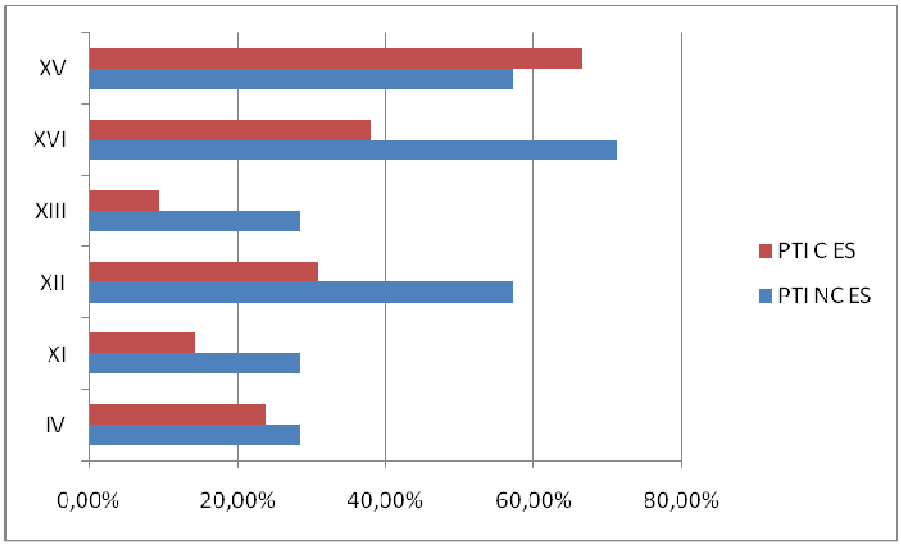
Considerando o percentual dos indivíduos que apagariam o email imediatamente (TABELA 1), é possível observar que a maioria (55,17% ; n = 32) oferece uma resistência aos e-mails considerados por eles duvidosos. Entretanto, essa atitude apesar de gerar proteção para o indivíduo, cria um problema em relação à possibilidade de divulgação de informações verdadeiras, as quais se encontram fora do conjunto de assuntos em que os indivíduos estão acostumados a tratar por email, gerando por exemplo, uma perda da possibilidade de realizar uma compra promocional que poderia ser do interesse do indivíduo e, ao mesmo tempo, diminui o número de possibilidade de vendas das empresas que trabalham o comércio eletrônico e/ou divulgam *e-mail marketing*.

Dos entrevistados, ainda em relação à pergunta apresentada na tabela 1, é possível notar que um valor de 39,66% dos indivíduos (n = 23) respondeu que "apontaria o mouse para o link sem clicar". A escolha dessa alternativa sugere que os mesmos indivíduos conheçam os meios utilizados para se reconhecer quando se trata efetivamente de *phishing*, pois ao passar o cursor sobre o link aparece a URL (endereço eletrônico do arquivo) permitindo verificar o real direcionamento do link.

Entretanto, cabe ressaltar que existem outras estratégias de ataque de *phishing*, como através de *sites* de relacionamentos, *iphishing* e *phishing* por mensageiros instantâneos, que não foram alvos de investigação no presente estudo, mas representam potenciais riscos à segurança da informação nas organizações.

Para avaliar se os profissionais de TI apresentam perfis capazes de gerar proteção das informações das organizações, foram aplicadas as seguintes perguntas: IV, XI, XII, XIII, XVI e XV (Anexo) e as comparações dos dados entre os grupos profissionais de TI que conhecem engenharia social (PTI C ES) e profissionais de TI que não conhecem engenharia social (PTI NC ES) estão resumidas no gráfico 1.

GRÁFICO1: Perfil dos profissionais de TI conhecedores e não conhecedores de engenharia social em relação aos cuidados com o uso e fornecimento de senhas



Como resultado dos profissionais de TI que responderam não conhecer engenharia social (n = 7) foi identificado que 28,56% (n = 2) desses ocupam cargos de nível gerencial, 28,56% (n = 2) afirmam que outro(s) funcionário(s) conhecem sua(s) senha(s) utilizadas na empresa, 57,12% (n = 4) afirmam já ter utilizado a senha de outros funcionários, 28,56% (n = 2) permitem que outras pessoas utilizem sua senha para algum tipo de trabalho rápido, 71,40% (n = 5) só alteram a senha quando o sistema solicita, 57,12% (n = 4) utiliza uma mesma senha para serviços diferentes e conhecem informações vitais para o negócio da empresa.

Em relação aos resultados obtidos com a aplicação das mesmas perguntas aos profissionais de TI conhecedores de engenharia social, os valores obtidos foram: 23,81% (n = 10) ocupam cargos de nível gerencial; 14,29% (n = 6) afirmam que outro(s) funcionário(s) conhecem sua(s) senha(s) utilizadas na empresa; 30,95% (n = 13) afirmam já ter utilizado a senha de outros funcionários; 9,52% (n = 4) permitem que outras pessoas utilizem sua senha para algum tipo de trabalho rápido; 38,10% (n = 16) só alteram a senha quando o sistema solicita e 66,67% (n =

28) utiliza uma mesma senha para serviços diferentes e conhecem informações vitais para o negócio da empresa.

Os dados apresentados sugerem uma elevada vulnerabilidade dos profissionais de TI, independente do fato serem conhecedores do tema engenharia social, permitindo considerar que os mesmos necessitem de capacitações contínuas para encarar de forma mais cuidadosa o manejo das ferramentas que permitem a proteção das informações, como por exemplo, suas senhas. Entretanto, a partir dos dados referentes à investigação sobre a permissibilidade da utilização de suas senhas por outros para a realização de trabalhos rápidos e a frequência com que alteram suas senhas é possível sugerir uma tendência a um comportamento mais protetor desempenhado pelos profissionais de TI que conhecem o tema engenharia social.

Tais resultados permitem sugerir que a participação de profissionais de TI conhecedores da engenharia social sejam essenciais para uma melhor percepção da realidade do nível de proteção das informações das instituições. Além disso, esses profissionais, uma vez capacitados, podem atuar no processo de disseminação do conhecimento sobre a engenharia social e sua técnicas, afim de aplicar uma efetiva política de segurança da informação.

5 CONCLUSÃO

Pode-se concluir a partir dos resultados, que na amostra o fator humano persiste como uma relevante fragilidade dentro da segurança da informação, uma vez que ainda existem profissionais não conhecedores da engenharia social nas organizações, os quais apresentam atitudes que colocam em risco a segurança das informações.

Outro aspecto relevante pode ser observado sobre os profissionais de TI conhecedores da engenharia social que, em menor escala, também chegam a desenvolver um comportamento capaz de torná-los vitimas da engenharia social, expondo assim as informações das organizações.

Dessa forma, conclui-se que com a crescente evolução dos sistemas e tecnologias de segurança da informação, os atacantes estão concentrando seus esforços no fator humano. Isso se dá devido o fato de que as pessoas são os elementos mais vulneráveis na gestão da segurança, pois são elas que executam e dão suporte aos processos de uma organização, e sempre estarão presentes nos

sistemas de segurança da informação, porém, não tem recebido a devida atenção e investimento por parte das organizações, por isso a maior parte dos incidentes envolvendo segurança da informação está diretamente ligada ao fator humano. Para amenizar estes riscos, as organizações devem criar políticas de segurança centralizadas e bem divulgadas para todos os seus colaboradores.

ANEXO 1

O questionário aplicado:

I. Qual sua idade?
II. Qual seu sexo?
III. Qual seu nível de instrução?
IV. Qual nível de sua função na empresa onde trabalha?
V. Em que área você trabalha?
VI. Quanto tempo você trabalha na empresa atual?
VII. Você possui outro emprego?
VIII. Você costuma abrir e-mails de pessoas desconhecidas?
IX. Você já recebeu e-mail sobre débitos, multas de veículos, solicitação de cadastros bancários ou conteúdo assemelhado?
X. Se você recebesse um e-mail informando sobre uma premiação e solicitando clicar sobre um link para maiores informações, o que faria?
XI. Alguém mais, além de você, conhece a(s) sua(s) senha(s) na empresa onde trabalha?
XII. Você já utilizou senha de outro funcionário?
XIII. Você permite que outras pessoas utilizem sua senha para algum tipo de trabalho rápido?
XIV. Você anota suas senhas em algum local próximo ao computador ou local de fácil acesso?
XV. Você utiliza uma mesma senha para serviços diferentes?
XVI. Com que frequência você altera sua(s) senha(s)?
XVII. Existe uma política para utilização de senhas fortes na empresa onde trabalha?
XVIII. Onde está sediada a empresa que você trabalha?
XIX. Qual a área de atuação da empresa onde trabalha?
XX. A empresa disponibiliza orientação sobre a divulgação de informação da mesma?
XXI. A empresa possui uma Política de Segurança da Informação?
XXII. A Política de Segurança da Informação é divulgada aos novos funcionários?
XXIII. A empresa possui um departamento de TI especializado?

XXIV. Existe alguma orientação de restrição quanto à utilização de e-mails, internet, telefone ou dispositivos de armazenamento portátil aos novos funcionários?

XXV. Os funcionários assinam algum termo de responsabilidade e/ou confidencialidade sobre as informações da empresa?

XXVI. Qual sua atitude ao receber solicitação de informação por telefone ou e-mail?

XXVII. Você conhece as informações vitais para o negócio da empresa?

XXVIII. Onde você guarda informações confidenciais?

XXIX. Existe controle de acesso à rede?

XXX. Há algum controle de acesso às aplicações ou diretórios?

XXXI. Há critérios para computação móvel e trabalho remoto?

XXXII. Enquanto trabalha, costuma ter algum papel em sua mesa com informações sobre a empresa ou cliente da empresa?

XXXIII. Ao sair, você costuma deixar sua mesa limpa, sem papéis importantes?

XXXIV. Ao sair, você costuma deixar seu computador bloqueado ou efetua logoff?

XXXV. O setor que trabalha, possui informações consideradas confidenciais?

XXXVI. Na sua opinião, todos os funcionários do seu setor sabem a importância das informações da empresa?

XXXVII. Você acha que seria difícil para pessoas externas, conseguirem informações importantes da empresa?

XXXVIII. Quais os tipos de informações você possui acesso (pode ter mais de uma resposta)?

XXXIX. Existe procedimento para cópias de segurança das informações?

XL. Você sabe o que é Segurança da Informação?

XLI. Você sabe o que é Engenharia Social?

REFERÊNCIAS

ALVES, Cássio B. **Segurança da informação vs. Engenharia Social:** Como se proteger para não ser mais uma vítima, 2010. Disponível em: <http://monografias.brasilescola.com/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm/>. Acesso em 02 dez. 2014.

BRAGA, Pedro H. C. **Técnicas de Engenharia Social,** 2010. Disponível em: < http://www.gris.dcc.ufrj.br/documentos/artigos/engenharia-social>. Acesso em 02 dez. 2014.

BALDIM, Natália P. **Engenharia Social e Segurança da Informação no Ambiente Corporativo:** uma análise focada nos profissionais de Secretariado Executivo, 2007. Disponível em: <http://www.secretariadoexecutivo.ufv.br/docs/anexo8.pdf>. Acesso em 01 abr. 2014.

CERUTTI, Fernando. **Necessidade e componentes gerais da segurança da informação,** 2012. Disponível em: < http://www.diegomacedo.com.br/necessidade-e-componentes-gerais-da-seguranca-da-informacao/>. Acesso em 02 dez. 2014.

COSTA, Josué. **Engenharia Social e Segurança da Informação na Gestão de Pessoas,** 2013. Disponível em: < http://www.administradores.com.br/artigos/tecnologia/engenharia-social-e-seguranca-da-informacao-na-gestao-de-pessoas/68812/>. Acesso em 02 dez. 2014.

FURTADO, Teresa. **O que é phishing e malware,** 2012. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-phishing-e-malware.html>. Acesso em 02 dez. 2014.

JUSTASKGEMALTO. **O que são esquemas de fraude via vishing, spoofing de identificador de chamada e phishing via SMS?**, 2014. Disponível em: <http://www.justaskgemalto.com/br/comunicando/tips/o-que-sao-esquemas-de-fraude-vishing-spoofing-de-identificador-de-chamada-e-phishin>. Acesso em 15 jul. 2014.

MARTINS, Elaine. **Cuidado com a engenharia social,** 2008. Disponível em: <http://www.tecmundo.com.br/msn-messenger/1078-cuidado-com-a-engenharia-social.htm>. Acesso em 02 dez. 2014.

MICROSOFT. **O que é engenharia social?**, 2014. Disponível em: <http://www.microsoft.com/pt-br/security/resources/socialengineering-whatis.aspx>. Acesso em 26 out. 2014.

MOREIRA, Ademilson. **A importância da segurança da informação,** 2012. Disponível em: <http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao >. Acesso em 02 dez. 2014.

NASSARO, Davies. **Engenharia Social:** Explorando o Fator Humano dos Sistemas de Segurança da Informação, 2012. Disponível em: <http://www.scribd.com/doc/244783660/engenharia-social-explorando-o-fator-humano-dos-sistemas-de-seguranc3a7ada-pdf >. Acesso em 02 dez. 2014.

OLHAR DIGITAL. **Cibercriminosos Usam Morte do Cantor Chorão para Espalhar Vírus,** 2013. Disponível em: < http://olhardigital.uol.com.br/noticia/cibercriminosos-usam-morte-do-cantor-chorao-para-espalhar-virus/33088>. Acesso em: 02 dez. 2014.

PEIXOTO, Mário. **Segurança da informação:** Vale muito aplicar a ISO 27002, 2012. Disponível em: < http://webinsider.com.br/2012/11/12/seguranca-da-informacao-vale-muito-aplicar-a-iso-27002/>. Acesso em 02 dez. 2014.

POPER, Marcos A.; BRIGNOLI, Juliano T. **Engenharia Social:** Um Perigo Eminente, 2002. Disponível em: <http://www.posuniasselvi.com.br/artigos/rev03-05.pdf>. Acesso em 02 dez. 2014.

SILVA FILHO, Antônio M. **Entendendo e Evitando a Engenharia Social:** Protegendo Sistemas e Informações, 2004. Disponível em: <http://www.espacoacademico.com.br/043/43amsf.htm/>. Acesso em 02 dez. 2014.

SILVA JUNIOR, Marcos Vinícius. **O que é segurança da informação?,** 2009. Disponível em: <http://webinsider.uol.com.br/2009/09/23/o-que-e-seguranca-da-informacao/>. Acesso em 03 jan. 2014.

WEBSEGURA.NET. **Phishing ao Banco Santander,** 2011. Disponível em: <http://www.websegura.net/tag/banco/>. Acesso em 02 dez. 2014.

WEINBERG, Neal. **5 dicas para evitar ataques de phishing direcionados a empresas,** 2013. Disponível em: <http://idgnow.com.br/ti-corporativa/2013/03/07/5-dicas-para-evitar-ataques-de-phishing-direcionados-a-empresas/>. Acesso em 02 dez. 2014.