A IMPORTÂNCIA DE UM PROGRAMA DE CONSCIENTIZAÇÃO NO ÂMBITO DO EXÉRCITO BRASILEIRO

Felipe Pereira Cyrino
Pós-graduado, Lato Sensu, de Especialização em Comunicações

RESUMO: Diante do cenário tecnológico moderno, no qual há um processo contínuo de inovação e integração de novos conceitos e capacidades, se percebe o que a informação se tornou o maior patrimônio da sociedade. O valor da informação no contexto moderno é tão grande, que ela se faz vital para qualquer instituição que se queira manter viva e competitiva. De tal maneira percebe-se que as instituições possuem um alto grau de dependência da informação. Essa dependência nos faz perceber que a Segurança da Informação é um pré requisito para qualquer instituição, inclusive para o Exército Brasileiro. Em contrapartida observa-se, no contexto atual, que a Engenharia Social é um dos fatores que mais comprometem não só a Segurança da Informação, mas também a segurança organizacional. A engenharia Social trata-se de uma técnica de intrusão que explora as fraquezas do ser humano, fazendo ou não o uso de tecnologias para a obtenção da informação. O presente estudo trata-se de uma revisão bibliográfica e documental que tem o objetivo geral verificar e compreender a Engenharia Social e destacar a importância de conscientização do tema no âmbito do Exército onde serão abordadas técnicas utilizadas pela Engenharia Social e medidas para combatê-la. Nesse contexto será observado, como resultado do estudo, a importância de um programa de conscientização para combater a Engenharia Social.

Palavras-Chave: Informação. Engenharia Social. Segurança da Informação.

1 INTRODUÇÃO

O presente estudo está inserido no campo da cibernética. De acordo com Morais (2006), cibernética pode ser definida como a “ciência da comunicação e do controle, seja do animal (homens, seres vivos), seja da máquina”.

Fazendo uma imersão no campo da cibernética, o presente trabalho tem como objetivo explorar o campo da engenharia social. O tema visou apontar a importância da conscientização e do treinamento para combater os ataques dos engenheiros sociais.

Atualmente o mundo é fortemente articulado por redes, devido aos grandes benefícios que são oferecidos pela alta tecnologia que está em constante desenvolvimento.

Nesse contexto, é possível perceber o valor que a informação adquiriu nos dias atuais; sendo ela de vital importância a qualquer instituição. Por esse motivo, a informação passou a merecer uma gestão mais específica que, entre outras coisas, contemplasse a garantia da segurança da informação.

Com relação à segurança da informação, se pode dizer que as instituições têm ciência e adquirem tecnologias de última geração para manterem a Informação segura. As intuições, ao investirem nessas tecnologias para segurança da informação, acabam esquecendo-se de um fator tão importante quanto à tecnologia, que é o fator humano.

O fator humano destaca-se como um importante elo para que exista a segurança da informação, já que é fato que grande parte dos vazamentos de informações das instituições ocorre por técnicas que conhecemos por Engenharia Social. (PEIXOTO, 2006)

Pode-se definir engenharia social como o conjunto de práticas que são utilizadas para a obtenção de informações valiosas e sigilosas das instituições por meio da vulnerabilidade humana, geralmente se utiliza da falta de conhecimento dos indivíduos ou do excesso de segurança dos mesmos.

A partir destes assuntos foi levantado o

seguinte questionamento com base no estudo dos conceitos de segurança da informação e engenharia social: Qual a importância da conscientização e do uso de medidas de defesa contra a engenharia social?

Assim sendo, o presente estudo apresenta ao efetivo do Exército Brasileiro embasamento teórico para entenderem como a engenharia social ataca e quais são os principais métodos utilizados pela mesma. O trabalho apresenta também as principais medidas de proteção da informação que podem ser utilizadas, a fim de que os militares possuam alguns artifícios para identificarem um ataque da engenharia social e tenham embasamento para se defenderem.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O presente estudo pretende integrar os conceitos básicos e a informação científica relevante e atualizada, a fim de fornecer subsídios suficientes para analisar, verificar e compreender a engenharia social e destacar a importância de conscientização do tema no âmbito do Exército.

1.1.2 Objetivos Específicos

A fim de viabilizar a consecução do objetivo geral de estudo, foram formulados objetivos específicos, de forma a desencadear logicamente o raciocínio descritivo apresentado neste estudo. Os seguintes objetivos específicos foram elencados:

a. compreender de que maneira o comportamento do homem afetam a proteção da informação;

b. conhecer conceitos e características da segurança da informação;

c. estudar conceitos e características da engenharia social;

d. identificar as principais ferramentas e técnicas utilizadas pela engenharia social;

e. Identificar as principais medidas que podem ser utilizadas para a proteção da informação.

1.2 PROCEDIMENTOS METODOLÓGICOS

A pesquisa é um estudo descritivo e bibliográfico, no qual através da leitura e revisão bibliográfica, responsáveis por fornecer a base teórica do trabalho, os elementos tidos como importantes serão expostos e analisados. Cabe ressaltar também que serão destacados alguns autores visando alcançar os objetivos propostos.

Ao término da revisão, por se tratar de um campo de investigação com produção de conhecimento já estudada antes, foram encontrados várias fontes de pesquisa de qualidade, visto que se trata de documentos importantes e autores renomados.

Amparados nessas fontes, iniciou-se a coleta de dados, baseada em leituras de livros, revistas e endereços eletrônicos. Na realização da pesquisa foi realizado um fichamento, devido ao grande número de informações levantadas, pois é um modo de armazenar essas informações que se faz muito útil quando existe a necessidade de recuperar um dado. Para isso, serão utilizadas fichas-resumo, nas quais vão se apresentar de maneira rápida e concisa as idéias do autor; e fichas de citação, onde serão transcritos fragmentos relevantes ao estudo.

O levantamento e a seleção da bibliografia, a coleta de dados, a análise dos dados, a leitura analítica, e a argumentação compõem o delineamento da pesquisa.

Para a realização da pesquisa bibliográfica, os trabalhos citados abaixo serviram como fonte de busca:

a. livros específicos focados em engenharia social e segurança da informação;

b. revistas;

c. artigos;

d. consulta a endereços eletrônicos es-

pecializadas no assunto.

2 FATOR HUMANO NO MANUSEIO DA INFORMAÇÃO

Em qualquer instituição, onde exista a preocupação com o manuseio e a segurança da informação, sempre existirá um fator que se destaca como um fator de desequilíbrio, o conhecido "fator humano". (MARCELO; PEREIRA, 2005).

De tal forma, é necessário que se reconheça a importância do elemento humano no trato com as informações, levando em consideração que o ser humano é o elo mais fraco da cadeia de segurança. Assim sendo, sobre o ser humano devem recair os principais cuidados durante as fases de especificação, implantação e gestão da segurança da informação. (PINHEIRO, 2008).

Como define Mitnick; Simon :

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003 apud ALVES, 2010, p. 14).

O fator humano está diretamente relacionado a uma grande parte de ataques promovidos contra a informação. A exploração das vulnerabilidades do ser humano é um ponto que deve ser levado em consideração em qualquer política de segurança da informação.

2.1 VULNERABILIDADES DO SER HUMANO

Como já foi dito, o ser humano é o elemento mais vulnerável de qualquer sistema de segurança da informação. São exatamente os traços comportamentais e psicológicos apresentados pelo ser humano que são explorados pela engenharia social.

Dentre essas características tornam o ser humano vulnerável, é possível destacar (JUNIOR, 2006):

- **vontade de ser útil**: Geralmente, o ser humano procura agir com cortesia e busca ajudar os outros quando se faz necessário;
- **busca de novas amizades**: Quando são elogiados, o ser humano costuma sentir-se bem, ficando assim mais vulnerável para fornecer informações;
- **prorrogação da responsabilidade**: Muitas vezes o ser humano considera que ele não é o único responsável por um conjunto de atividades ou responsabilidades;
- **persuasão**: É compreendida como a arte de persuadir pessoas, onde se busca respostas específicas para determinado objetivo; e
- **autoconfiança**: Como próprio nome diz, é o fato que a maioria das pessoas não se consideram ingênuas a ponto de serem enganadas e utilizadas de alguma maneira.

Existem inúmeros outros fatores que ainda podem ser considerados vulnerabilidades do ser humano. Em razão destes fatores, é possível entender que sempre haverá brechas de segurança da informação, uma vez que a manipulação das informações é feita por indivíduos.

3 SEGURANÇA DA INFORMAÇÃO

De acordo com Peixoto (2006, apud ALVES, 2010, p. 17), "O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos,

modificações não autorizadas ou até mesmo sua não disponibilidade".

A segurança da informação é dividida em três pilares ou princípios básicos, que são definidos por Peixoto (2006) da seguinte maneira:

- **confidencialidade**: É a garantia que as informações chegarão ao seu destino sem que se dissipem para outros meios ou lugares onde não deveriam passar;
- **integridade**:É a garantida de que as informações não sofreram nenhuma alteração durante o trajeto entre o remetente e o destinatário; e
- **disponibilidade**: A informação deve estar sempre disponível aos seus usuários no momento em que estes necessitarem. Peixoto (2006) entende que nada adianta ter confidencialidade e integridade se a informação não estiver disponível.

Em resumo, segurança da informação pode ser compreendida como as políticas, procedimentos e medidas técnicas usadas para impedir o acesso não autorizado a um sistema de informação.

3.1 VULNERABILIDADES DA SEGURANÇA DA INFORMAÇÃO

Podemos compreender vulnerabilidade da segurança da informação como uma fragilidade da segurança da informação, ou simplesmente como pontos mais suscetíveis a serem expostos a danos.

Os principais tipos de vulnerabilidades existentes na segurança da informação, de acordo com Peixoto (2006) são classificadas da seguinte forma:

- **físicas**: São constituídas por instalações com estruturas de segurança fora dos padrões mínimos, como exemplo uma sala de CPD mal planejada;
- **naturais**: São as causadas por fenômenos naturais, como tempestades, incêndios, desabamentos, além da falta de energia;
- **hardware**: São os desgastes causados nos equipamentos por obsolescência ou má utilização;
- **software**: São constituídos pela má instalação, pelo vazamento de informações, pela perda de dados ou pela indisponibilidade de recursos;
- **mídias**: Fontes de armazenamento de mídias podem ser perdidas ou danificadas;
- **comunicação**: Constituídos por acessos não autorizados ou pela perda de comunicação; e
- **humanas**: São as vulnerabilidades que se referem ao fator humano que são exploradas pelas técnicas da engenharia social.

Ainda sobre o tema, Peixoto (2006) diz que geralmente as empresas ou instituições não adotam potencial investimento em segurança digital mais especificamente na segurança das informações.

4 ENGENHARIA SOCIAL

Campos (2007) define a engenharia social como de uma técnica utilizada para que se obtenha acesso a informações, onde ,substancialmente, um indivíduo se utiliza de métodos para induzir uma pessoa a quebrar protocolos e procedimentos de segurança.

Nakamura e Geus (2003) definem engenharia social da seguinte forma:

> A engenharia social é a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem

> senhas ou outras informações que possam comprometer a segurança da organização. (NAKAMURA,GEUS, 2003, p.70).

Pode-se definir engenharia social como o conjunto de práticas que são utilizadas para a obtenção de informações valiosas e sigilosas das instituições por meio da vulnerabilidade humana, geralmente se utiliza da falta de conhecimento dos indivíduos ou do excesso de segurança dos mesmos.

Mostrando a importância que deve ser dada a engenharia social, Peixoto (2006) afirma que a dentre as vulnerabilidades encontradas na segurança da informação a engenharia social está inserida como um dos desafios (senão o maior) mais complexos e que merecem total atenção.

4.1 FERRAMENTAS UTILIZADAS PELO ENGENHEIRO SOCIAL

O engenheiro social realiza seus ataques fazendo uso de ferramentas comuns presentes no nosso dia a dia e que muitas vezes passam despercebidas por todos.

Dentre as principais ferramentas que são utilizadas pelos engenheiros sociais podemos destacar: (PEIXOTO, 2006)

- **telefone ou Voip**: Se passar por alguém que não é seria um dos típicos ataques de engenharia social;
- **internet**: através de sites que forneçam informações sobre a pessoa (facebook);
- **intranet**: Por exemplo, por acesso remoto, capturando-se o micro de determinado usuário da rede e se passando por alguém que na verdade não é;
- **e-mail** (Fakemail, e-mails falsos, os famosos phishing scan);
- **pessoalmente**: Fazer uso do poder de persuasão, da habilidade de saber conversar;
- **fax**: É necessário obter o número do fax antes para depois iniciar o ataque;
- **cartas/correspondência**: Embora não seja muito utilizado atualmente, esse recurso funciona muito bem com pessoas mais velhas;
- **spyware**: Software “espião” usado para monitorar de modo oculto as atividades do computador de um alvo;
- **mergulho no lixo**: Muitas vezes aquilo que é descartado no lixo de maneira indevida, pode possuir informações que serão usadas pelo engenheiro social contra a vítima; e
- **surfar sobre os ombros**: Nada mais é que observar as pessoas digitando no computador informações como senhas e usuários e assim conseguir roubá-las.

Existem várias ferramentas que podem ser usadas para os ataques dos engenheiros sociais. No uso destas ferramentas o Engenheiro Social se utiliza de algumas técnicas simples, que serão exploradas adiante.

4.2 TÉCNICAS UTILIZADAS PELO ENGENHEIRO SOCIAL

Aliadas ou uso das ferramentas, mostradas anteriormente, os engenheiros sociais se utilizam de técnicas onde procuram explorar a vulnerabilidade humana, sempre possuindo uma resposta ao possível comportamento humano apresentado pela vítima.

De acordo com Peixoto (2006), os engenheiros sociais sempre se utilizam de técnicas clássicas. A seguir serão mostradas algumas dessas técnicas.

4.2.1 Informações Inofensivas x Valiosas

Basicamente funciona como um quebra-cabeça. As informações são obtidas em pedaços e quando juntados resultarão na “figura completa”. Sendo assim informações que em

uma primeira impressão parecem irrelevantes, quando reunidas com outras informações também consideradas irrelevantes, podem dar origem a uma informação de grande valia.

Ainda, concordando com Peixoto (2006), é necessário avaliar todo repasse de informação, levando em consideração quem está solicitando e a real necessidade desta pessoa saber da informação.

4.2.2 Criando Confiança

Essa técnica utilizada pela engenharia social trata-se basicamente de adquirir primeiramente a confiança, reforçar esse vínculo de amizade aumentando ainda mais a confiança, para então começar a atacar e conseguir as informações julgadas necessárias.

De acordo com Peixoto (2006), o engenheiro social se prepara para responder todas as perguntas e indagações que podem acontecer, sem demonstrar nervosismo, sem gaguejar ou sem demonstrar insegurança de forma que a vítima não desconfie de nada.

4.2.3 Simplesmente Pedindo

A referida técnica é considerada a mais simples utilizada para se obter uma informação. Quando existe uma dúvida o natural é perguntar, ou seja, pedir a resposta.

De acordo com Peixoto (2006), para que a técnica tenha sucesso é necessário que o engenheiro social tenha conhecimento da linguagem e da estrutura do ambiente onde pretende fazer o ataque.

Em uma entrevista para a Information Week Brasil, Kevin Mitnick (2003) afirma que as duas características que são mais utilizadas nessa técnica são a autoridade e o medo. A autoridade transmite segurança no momento em que o engenheiro social demonstra que sabe o que está falando, o que faz a vítima se sentir sufocada e fornecer a informação desejada. Isso também acontece pelo fator do medo.

4.2.4 Engenharia Social Inversa

Essa técnica se baseia, basicamente, na criação de um problema pelo engenheiro social que somente ele conseguirá resolver. Dessa forma, o engenheiro social ganha confiança do alvo conseguindo convencer que existe um problema ou que o problema esta prestes a acontecer. Em seguida o atacante se apresenta como a pessoa certa que pode resolver problema. (MITNICK e SIMON, 2003 apud PEIXOTO, 2006).

Essa técnica é muito eficiente, pois o engenheiro social ganha a confiança da vítima, facilitando a obtenção das informações que realmente o atacante deseja.

5 MEDIDAS DE DEFESA CONTRA ENGENHARIA SOCIAL

Um dos maiores especialistas nesse assunto, Kevin Mitnick, é citado por Peixoto (2006) e afirma que: “A verdade é que não existe tecnologia no mundo que evite o ataque de um Engenheiro Social.” (MITNICK e SIMON, 2003 apud PEIXOTO, 2006, p. 56)

Em seu artigo, Filho (2004) considera que a medida que a o papel da informação na sociedade aumenta e ganha importância, a engenharia social se torna uma das principais ameaças de segurança das organizações. Com isso existem algumas medidas simples que podem ser tomadas para se defender ou evitar um ataque de engenharia social em uma organização. São elas:

- **educação e treinamento**: As pessoas devem ter consciência sobre o valor da informação que elas manipulam. Devem ser apresentados conceitos e as ferramentas e os métodos utilizados pela engenharia social;
- **segurança física**: Somente pessoas autorizadas devem ter acesso a determinadas dependências de uma organização e sempre que possível devem ser usados o monitoramento por câmeras das entradas da depen-

dência;

- **política de segurança**: São instruções claras que fornecem uma orientação para preservar informações; e
- **controle de acesso**: Os mecanismos de controle e acesso têm como objetivo evitar que usuários sem permissão possam ter acesso a informações ou a equipamentos.

O sucesso dos ataques da engenharia social pode acontecer em qualquer nível de comando das organizações, independentemente do investimento em realizado em segurança. O engenheiro social visa o atacara o fator humano e é um grande erro supor que qualquer um está imune. (GARTNER, 2002).

6 TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA

Ao se falar sobre o desenvolvimento de um programa de conscientização é pensado em tecnologias e estruturas físicas, porém não se pode deixar de lado o fator mais importante de todos que é o fator humano.

Um programa de conscientização sobre segurança da informação tem o objetivo principal influenciar os integrantes de uma organização a mudarem seus hábitos e atentarem para a importância da segurança da informação. (FONSECA, 2009)

Aliados ao programa deverão ter as políticas de segurança, e principalmente o treinamento do pessoal, que é um fator essencial para se alcançar sucesso em questão de segurança. (PEIXOTO, 2006)

Os treinamentos dos integrantes devem levá-los a criarem a percepção automática de quais informações devem ser protegidas e como adotar medidas simples para protegê-las e também devem fazer com que os integrantes consigam perceber ou identificar um ataque de engenharia social. (FONSECA, 2009)

Vale ressaltar, de acordo com Gartner (2002), afirma que uma política de segurança desatualizada ou surrealista leva os integrantes a negligenciá-las, o que dificulta o reconhecimento de um ataque de engenharia social.

Um bom e objetivo programa de treinamento e conscientização sobre segurança da informação, levando em consideração os aspectos do comportamento humano, devem levar em consideração alguns tópicos como os descritos por Mitnick e Simon (2003, apud PEIXOTO, 2006) e por Fonseca (2009). São eles:

- descrever a forma com que engenheiros sociais utilizam suas habilidades para enganar as pessoas;
- como reconhecer um possível ataque de Engenharia Social, identificando ferramentas e métodos utilizados pelos atacantes;
- o procedimento quando se desconfiar de alguma solicitação suspeita;
- a importância de questionar solicitações, independente do cargo, função ou importância que o solicitante possui;
- o fato de não confiar em pessoas que fazem solicitações de informações, sem antes fazer uma verificação adequada da identidade e autoridade da pessoa que deseja a informação;
- como proceder para a proteção de informações sigilosas;
- sintetizar e explicar cada ação da política de segurança, como exemplo, as mediadas de defesa quanto com o lixo ou a criação de senhas;
- a obrigação de cada integrante atender as políticas e as consequências do não atendimento;
- melhores práticas no uso do correio eletrônico, alertando para os vírus e armadilhas em geral;
- questões físicas de segurança;

- eliminação de documentos que contenham informações sigilosas independentemente se sua natureza é física ou eletrônica; e
- fornecer periodicamente material informativo, como por exemplo, lembretes (de preferência curtos e que chamem atenção).

Ainda sobre a conscientização e treinamento, Mitnick (2003) afirma que é interessante que se realizem testes com o objetivo de encontrar falhas ou descumprimento de alguma norma. Deve ser avisado aos integrantes da instituição que os testes serão realizados periodicamente.

Um programa de treinamento e conscientização se resume, basicamente, em uma reeducação de todos os integrantes da instituição, inserindo cada vez mais a cultura de segurança da informação. (FONSECA, 2009)

Todos os integrantes de uma instituição devem ser treinados e tem a consciência da importância da segurança da informação. A defesa mais forte contra os ataques de engenharia social é o fator humano estar bem treinado.

A conscientização e o treinamento devem existir sempre. Os integrantes devem sempre ser lembrados da possibilidade de sofrer ataque e de como evitá-los ou de como reagir diante de um.

7 CONCLUSÃO

O presente trabalho teve como objetivo geral aprofundar o tema Engenharia Social e alertar para a importância da conscientização do tema no âmbito do Exército.

Como objetivos específicos foram buscados um melhor entendimento sobre o que é Engenharia Social e Segurança da Informação, de forma que fossem enumeradas algumas medidas para a prevenção de ataques de engenheiros sociais.

Na conjuntura atual, é possível percebermos que o trâmite de informações se tornou muito mais veloz e que houve um grande aumento no fluxo da informação transitada. Sendo assim, a informação ganhou cada vez mais importância e é fundamental saber proteger as informações, principalmente aquelas restritas que o Exército possui.

À medida que o avanço da tecnologia permitiu um ganho de tempo e uma maior eficiência para a tomada de decisões por parte das instituições, como no caso do Exército Brasileiro, percebemos que tal avanço, também permitiu que fossem abertas novas portas para ações externas contra as informações. Observamos então, a importância que deve ser dada a segurança da informação.

O fator humano está diretamente relacionado com a segurança da informação, isto porque o manuseio da informação passa pelas mãos das pessoas da instituição. A segurança da informação começa e termina nas pessoas. Investir em tecnologia e deixar de lado o fator humano é um erro grave. É justamente nesse ponto que atua a Engenharia Social, explorando as vulnerabilidades humanas para adquirirem informações que julguem interessantes.

A engenharia social é definida basicamente como a exploração das vulnerabilidades humanas, através de métodos e ferramentas, para a obtenção de informações. Como disse Peixoto (2006), a engenharia social está inserida como um dos desafios (senão o maior deles) mais complexos no âmbito da segurança da informação.

Para inibir os ataques dos engenheiros sociais ou diminuir a efetividade dos mesmos, o Exército Brasileiro assim como qualquer instituição deve adotar estratégias tanto no nível físico (nos meios pelos quais o engenheiro social atua) quanto no nível psicológico (manipulando emoções).

A criação de um programa de conscientização em segurança, aliado as normas de segurança e da sua divulgação, faz com que os integrantes da instituição compreendam a importância da segurança da informação; quais

devem ser os cuidados no manuseio na informação; quais informações são sigilosas e quais são de caráter ostensivo; e quais medidas devem ser tomadas em caso de suspeita de ataque de um engenheiro social.

Aliados a esse programa de conscientização, deve estar algo que sem sombra de dúvidas é fundamental para combater ataques de engenharia social: o treinamento. Todas as pessoas que tem contato ou trabalham diretamente no manuseio de informações, principalmente sigilosas, devem passar por um treinamento para aprender a identificar os métodos e ferramentas utilizados no ataque de um engenheiro social e como irá reagir diante de um possível ataque.

Observamos também que uso de medidas simples de proteção já dificulta e muito o trabalho realizado pelo engenheiro social. O controle e acesso das áreas que manipulam informações sigilosas; a preocupação com a segurança física; a criação de uma política de segurança; a preocupação com o lixo; o simples uso de antivírus; e a preocupação em estabelecer uma senha segura, são exemplos de algumas medidas que defende uma instituição de um possível ataque.

Mas o principal inibidor de ataques de engenheiros sociais é sem dúvida a conscientização e o treinamento. O treinamento deve fazer a pessoa aprender a identificar os tipos de ataque e como reagir a cada um deles. Concordamos com Kevin Mitinick (2003) em que não existe tecnologia que evite um ataque de engenheiro social, portanto o treinamento contínuo é essencial para que as pessoas possam conhecer e estejam sempre preparadas para lidar com possíveis ataques.

O estudo do assunto não se esgotou totalmente neste trabalho, uma vez que este não era nosso objetivo. Este trabalho serve como um estudo preliminar para que novos trabalhos possam ser feitos a fim de aprofundar, discutir e padronizar processos e controles para inibir os ataques dos engenheiros sociais.

No final da pesquisa podemos observar a importância da conscientização dos militares do Exército, assim como em qualquer instituição, sobre a engenharia social, abordando técnicas e ferramentas utilizadas. Observamos também a importância de existir o treinamento do pessoal para evitar ataques.

O trabalho atingiu o objetivo estabelecido, que era colaborar como um meio de conscientização a respeito do tema proposto. Inserido no campo da cibernética, o trabalho apresentou conceitos sobre a Engenharia Social e mostrou que por mais tecnologia que exista na segurança da informação, continua sendo o ser humano o fator mais crítico e vulnerável. Foram abordadas também algumas medidas de simples adoção para o combate da Engenharia Social.

Conclui-se então que para proteger as informações das ações da Engenharia Social, é interessante que o Exército incentive uma cultura de conscientização sobre o tema, e que mantenha sempre atualizada, além de realizar treinamentos com as pessoas que manipulam as informações sigilosas, para que não exista perda ou vazamento de informações.

Não existe uma fórmula mágica para tornar um ambiente que manipula informação totalmente seguro. O conhecimento das técnicas da Engenharia Social, através de um programa de conscientização; e de medidas para evitar ataques de engenheiros sociais, ensinadas e reforçadas através dos treinamentos, são fundamentais para que o Exército Brasileiro consiga inibir vazamentos ou perdas de informações, obtidas através da Engenharia Social.

SOCIAL ENGINEERING:THE IMPORTANCE OF A CONSCIENTIZATION PROGRAM IN THE FRAMEWORK OF THE BRAZILIAN ARMY

ABSTRACT: Faced with the modern technological scenario, in which there is a continuous process of innovation and integration of new concepts and capacities, one realizes what information has become the greatest patrimony of society. The value of information in the modern context is so great that it becomes

vital to any institution that wants to stay alive and competitive. In such a way it is perceived that the institutions possess a high degree of dependence of the information. This dependence makes us realize that Information Security is a prerequisite for any institution, including for the Brazilian Army. On the other hand, it is observed in the current context that Social Engineering is one of the factors that most compromise not only Information Security, but also organizational security. Social engineering is an intrusion technique that exploits the weaknesses of the human being, whether or not the use of technologies to obtain information. The present study is a bibliographical and documentary review that has the general objective to verify and to understand the Social Engineering and to emphasize the importance of raising awareness of the subject within the scope of the Army where the techniques used by Social Engineering will be approached and measures to combat it. In this context, it will be observed, as a result of the study, the importance of an awareness program to combat Social Engineering.

Keywords: Information, Social Engineering, Information Security.

REFERÊNCIAS

ALVES, Cássio Bastos. **Segurança da Informação VS. Engenharia Social**: Como se proteger para não ser mais uma vítima. 63f. Brasília, 2010. Disponível em: < http://www.administradores.com.br/_resources/files/_modules/academics/academics_3635_20101207234707794d.pdf > Acesso em: 05 abril de 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: informação e documentação: referências - elaboração. Rio de Janeiro, 2002.

_____. **NBR 10520**: citação em documentos. Rio de Janeiro, 2002.

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do Hacker Ético**. 4ª edição rev. e ampl. Florianópolis: Visual Books, 2011.

ESCOLA DE COMUNICAÇÕES. Seção de Pós-Graduação e Doutrina. **Extrato do Manual de Metodologia da Pesquisa, confeccionada pelo Centro de Estudos de Pessoal (CEP) ao Curso de Psicopedagogia e Orientação Educacional pela Professora Maria Christina Zentgraf**. Brasília, 2017.

FERREIRA, Aurélio B. de Holanda. **O mini dicionário da língua portuguesa**. 4ª edição revista e ampliada do mini dicionário Aurélio. 7ª impressão – Rio de Janeiro, 2002.

FILHO, Antônio Mendes da Silva. **Segurança da Informação**: Sobre a Necessidade de Proteção de Sistema de Informações in Revista Espaço Acadêmico nº42 – novembro de 2004; Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm> Acesso em: 02 maio de 2017.

FONSECA, Paula F. **Gestão de Segurança da Informação**: O Fator Humano. 2009. 16 f. Monografia (Especialização)– Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf > Acesso em: 12 abr. 2017.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**: o usuário faz a diferença. 1. ed. São Paulo: Saraiva, 2006.

GANDINI, J. A. D.; SALOMÃO, D. P. S.; JACOB, C. **A segurança dos documentos digitais**. Revista Jurídica: Órgão Nacional de Doutrina, Jurisprudência, Legislação e Crítica Judiciária, Porto Alegre, Ano 53, v. 50, n. 295, p. 59-71, mai. 2002.

GARTNER, INC. **Protect Against Social Engineering Attacks**. Gartner's Information Security Strategies Research, Volume 1, Issue 1, February 2002; Disponível em: <http://www.gartner.com/gc/webletter/security/issue1/article2.html> Acesso em 10 maio. 2017

GONÇALVES, L. R. O. **Um modelo para verificação, homologação e certificação de aderência a norma nacional de segurança da informação – NBR-ISSO / IEC- 17799**. 189f. Tese (Mestrado em Ciências em Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro, COPPE – Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Rio de Janeiro, 2005.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social.** [S.l.: s.n.], 2006, Disponível em: <http://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social>. Acesso em: 17 abr. 2017.

LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. Revista Economia & Tecnologia, Paraná, v. 8, n. 3, p. 38-44, jan./mar. 2005.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de In-**

formação Gerenciais: administrando a empresa digital. 5ª ed. São Paulo: Person Pretice Hall, 2004.

MARCELO, Antônio; PEREIRA, Marcos. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005.

MITNICK, Kevin D.; SIMON, Willian L. **A arte de enganar: Ataques de Hackers**: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

MORAIS, Catiane Pimentel De. **Cibernética, Teoria Matemática e Teoria dos Sistemas**. 2006. Disponível em <http://www.zemoleza.com.br/trabalho-academico/humanas/contabilidade/cibernetica-teoria-matematica-e-teorias-dos-sistemas> Acesso em: 23 Mai 17.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes em ambientes Cooperativos**. Editora Futura; 2003

PEIXOTO, Márcio C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**.1ª ed. Rio de Janeiro: Brasport, 2006.

PINHEIRO, José Maurício. **Biometria nos Sistemas Computacionais – Você é a Senha**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva da segurança da informação. 9ª reimpressão. Rio de Janeiro: Elsevier, 2003

SILVA FILHO, Antonio Mendes Da. **Segurança da Informação**: Sobre a Necessidade de Proteção de Sistemas de Informações. Revista Espaço Acadêmico Nº42/2004. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm> Acesso em: 10 Fev. 2017.

SIQUEIRA, Marcelo Costa. **Gestão Estratégica da Informação**. Rio de Janeiro: Brasport, 2005.

YAMAGISHI, T. **Trust and social intelligence**: the evolutionary game of mind and society. Tóquio: Tokyo University Press, 1998.

ZAPATER, Márcio; SUZUKI, Rodrigo. **Segurança da Informação**: Um diferencial determinante na competitividade das corporações. São Paulo: Promon, 2005.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). 1° Tenente da Arma de Artilharia do Exército Brasileiro da turma de 2013. Concluiu com aproveitamento o curso de Operação do Sistema de Mísseis e Foguetes no Centro de Instrução de Mísseis e Foguetes. É pós-graduado pela Escola de Comunicações, *Lato Sensu*, em Oficial de Comunicações. Atualmente, exerce a função de Chefe do Centro de Operações de Apoio Logístico do Centro de Logística de Mísseis e Foguetes e pode ser contactado pelo email felipereira.art@gmail.com.