ATAQUES DE ENGENHARIA SOCIAL: MEDIDAS PREVENTIVAS PARA A SEGURANÇA DA INFORMAÇÃO.

MATHEUS MURARI AZZOLIN
Pós-graduado, Lato Sensu, de Especialização em Comunicações

RESUMO: A PRESENTE PESQUISA CIENTÍFICA TEM COMO TEMA OS ATAQUES DE ENGENHARIA SOCIAL CONTRA AS ORGANIZAÇÕES MILITARES E SEUS MILITARES. O TRABALHO TEM O OBJETIVO DE LEVANTAR AS MEDIDAS PREVENTIVAS (PARA ELABORAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO) CAPAZES DE EVITAR ATAQUES DE ENGENHARIA SOCIAL CONTRA AS ORGANIZAÇÕES DO EXÉRCITO BRASILEIRO E OS MILITARES QUE NELAS SERVEM. PARA QUE FOSSE POSSÍVEL LEVANTAR TAIS MEDIDAS PREVENTIVAS, FOI REALIZADO UM TRABALHO DE PESQUISA BIBLIOGRÁFICA ACERCA DAS AMEAÇAS DE ENGENHARIA SOCIAL E PRINCIPAIS VULNERABILIDADES DAS OM. TAMBÉM FOI NECESSÁRIO UM ESTUDO SOBRE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, COM A FINALIDADE DE SELECIONAR MELHORES AÇÕES, DIRETRIZES E NORMAS CAPAZES DE EVITAR ATAQUES DESSA NATUREZA. COMO RESULTADO, O TRABALHO CIENTÍFICO MOSTRA QUAIS AS MEDIDAS PREVENTIVAS DEVEM SER CONSIDERADAS PARA A CORRETA SEGURANÇA DO ATIVO DE INFORMAÇÃO EM RELAÇÃO À ENGENHARIA SOCIAL. AO FIM, EXPÕE COMO ESSAS MEDIDAS DEVEM SER ABORDADAS PARA A MELHOR CONSCIENTIZAÇÃO DO PÚBLICO INTERNO E APRESENTA OUTRAS CARACTERÍSTICAS INDISPENSÁVEIS A UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO. O CONTEÚDO APRESENTADO TORNA A PESQUISA RELEVANTE, AO CONTRIBUIR PARA SINTETIZAR MEDIDAS PREVENTIVAS DE ATAQUES DE ENGENHARIA SOCIAL, VOLTADAS ESPECIFICAMENTE, PARA O MEIO MILITAR E COLABORAR ASSIM, PARA A MELHORIA DAS POLÍTICAS DE CONSCIENTIZAÇÃO DOS MILITARES E PROTEÇÃO DAS INFORMAÇÕES.

PALAVRAS-CHAVE: MEDIDAS PREVENTIVAS. ENGENHARIA SOCIAL. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

1 INTRODUÇÃO

A cibernética segundo o dicionário Michaelis (2017) é a "ciência cujo objeto de estudo concentra-se na comparação dos sistemas e mecanismos de controle automático, bem como na regulação e comunicação não só nos seres vivos, porém também nas máquinas".

Dentro do campo extenso da cibernética, o presente estudo se concentra nas ameaças de engenharia social contra as Organizações Militares (OM) do Exército Brasileiro (EB). O tema explora a importância de se considerar medidas para prevenir ataques de engenharia social contra OM e seus militares em uma Política de Segurança da Informação (PSI).

A ocorrência de crimes digitais vem aumentando muito, principalmente na última década. Reflexo da evolução constantes das tecnologias e da maior quantidade de máquinas e redes presentes em instituições que dependem cada vez mais do emprego desses meios para sobreviver.

Portanto, é necessário que as medidas de segurança se tornem, cada vez mais, parte da rotina dos funcionários de uma instituição que busca a salvaguarda dos seus dados:

> Dentre os fatos que demonstram o aumento da importância da segurança, pode-se destacar a rápida disseminação de vírus e worms, que são cada vez mais sofisticados. Utilizando técnicas que incluem a engenharia social, [...] os ataques visam a contaminação e a disseminação rápida, além do uso das vítimas como origem para novos ataques (NAKAMURA E GEUS, 2007, p. 27).

Ataques de engenharia social são lançados na tentativa de obter informações para a prática de crimes contras as instituições ou seus funcionários.

Por isso, o artigo tem a seguinte hipótese: as medidas preventivas para evitar ataques de engenharia social às OM e seus militares são indispensáveis em uma Política de Segurança

da Informação (PSI).

A pesquisa buscou levantar as medidas preventivas que visam impedir tanto a obtenção de dados e informações das OM (sejam elas do viés operacional, administrativo ou da segurança orgânica), quanto o vazamento de informações que tornem os militares e suas famílias vulneráveis a ataques de engenharia social.

O artigo se justifica por levantar as medidas preventivas de ataques de engenharia social, voltadas especificamente, para o meio militar, colaborando para a melhoria das políticas de segurança da informação das OM.

1.1 OBJETIVOS

O objetivo geral é levantar quais são as medidas a serem consideras para a elaboração de uma política de segurança da informação a fim de evitar ataques de engenharia social contra as OM e seus militares.

Foram formulados os seguintes objetivos específicos:

a) descrever o que é engenharia social e como ocorre um ataque;

b) descrever o que é uma política de segurança da informação;

c) elencar e descrever quais são as principais ameaças de engenharia social às OM;

d) elencar as medidas que devem ser consideradas para a elaboração de uma política de segurança da informação.

1.2 PROCEDIMENTOS METODOLÓGICOS

Ao apresentar medidas preventivas para elaborar uma política de segurança da informação a fim de impedir ataques de engenharia social este artigo busca soluções práticas para problemas concretos. Portanto, em relação à natureza, ele pode ser classificado como uma pesquisa aplicada e de abordagem qualitativa.

Por ter sua execução pautada na obtenção de informações já existentes em outros documentos, publicações, artigos e reportagens, o presente artigo é classificado como uma pesquisa bibliográfica.

Para o subsídio bibliográfico as fontes de consulta selecionadas foram de instituições públicas e privadas que possuem atividades voltadas ao combate à engenharia social e elaboração de políticas de segurança da informação. Foram consideradas fontes de especialistas no assunto, documentários, reportagens e documentos relacionados ao tema.

O desencadeamento lógico do desenvolvimento pretende abordar os tópicos previamente definidos nos capítulos:

a) POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - define o que é uma política de segurança da informação;

b) ENGENHARIA SOCIAL – descreve de forma pormenorizada o entendimento sobre a engenharia social e as ameaças às OM;

c) MEDIDAS PREVENTIVAS – esse capítulo apresenta as medidas preventivas contra ataques de engenharia social às OM e seus militares.

2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

2.1 INFORMAÇÃO

Para esta pesquisa considerou-se a seguinte definição de Raphael Mandarino (2009): “Infraestrutura Crítica da Informação é o subconjunto dos ativos de informação que afetem diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade”.

Ou seja, os ativos de informação podem ser definidos como todas as informações que de posse de alguém mal intencionado possam afetar as missões de uma OM e a segurança dos militares que trabalham nesse local.

2.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para Fontes (2006) segurança da informação "é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada".

Uma PSI é importante, pois, segundo Nakamura e Geus (2007, p.27) "[...] quando o profissional não conhece os riscos, ele tende a achar que tudo está seguro com o ambiente. Com isso, a organização passa, na realidade, a correr riscos ainda maiores, que é o resultado da negligência".

De acordo com Nakamura e Geus (2007, p.73) "[...] os aspectos humanos, sociais e pessoais não podem ser esquecidos na definição da estratégia de segurança". É justamente esse aspecto humano que dá origem aos ataques de engenharia social, que se aproveitam da má gestão da informação e fragilidades dos funcionários para causar diversos danos às organizações e, principalmente, às pessoas que fazem parte delas.

Por isso, é extremamente necessário que uma PSI contemple as medidas preventivas contra engenharia social.

3 ENGENHARIA SOCIAL

3.1 DEFINIÇÕES

Existem diversas técnicas para a obtenção de informações e invasão de sistemas. Umas das mais utilizadas é a engenharia social:

> A engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança (NAKAMURA E GEUS, 2007).

De acordo com Assunção (2011, p. 30), entre os fatores que tornam as redes inseguras o fator humano, justo o não técnico, é o pior deles:

> Através de técnicas de Engenharia Social, a manipulação do fator humano causa enormes desastres como: fazer um usuário rodar um cavalo de tróia sem saber, conseguir informações privilegiadas sobre empresas, obter especificações de um novo produto, etc. [...] (ASSUNÇÃO, 2011, p. 31).

De acordo com a definição de Nakamura e Geus, a engenharia social visa também, por meio da manipulação "quebrar procedimentos de segurança". É possível inferir que se trata de sua utilização para abrir brechas nos sistemas e obter a informação por meio de outras ferramentas, como a instalação de vírus:

> O fato mais recente envolvendo a engenharia social é sua ampla utilização em busca de um maior poder de disseminação de vírus. Procurando ludibriar os usuários para que abrissem arquivos anexados, vírus como o I Love You, Anna Kournikova e Sircam espalharam-se rapidamente pelo mundo (NAKAMURA E GEUS, 2007, p. 86).

A engenharia social também é utilizada quando a obtenção da informação só pode ser feita por meio do contato pessoal (como por exemplo, a rotina da OM ou horário de saída de uma viatura) ou de forma física (informações que não se encontram em bancos de dados virtuais, somente em pastas e arquivos físicos).

3.2 ATAQUES DE ENGENHARIA SOCIAL

3.2.1 Engenheiros sociais

O engenheiro social utiliza os sentimentos para manipular as pessoas e obter a informação que deseja. Porém, isso não significa que ele não tem conhecimento na área de cibernética, mas sim que ele apenas utiliza a engenharia social como uma de suas várias ferramentas para conquistar seus objetivos (NAKAMURA E GEUS, 2007, p. 85).

Os engenheiros sociais podem ter diversos motivos para realizarem um ataque. Normalmente tem a intenção de realizar ações para obter vantagens financeiras por meio de crimes, como o estelionato e furto. Porém, podem existir outras motivações, tais como, o sentimento de vingança contra algum militar ou contra a instituição, autoafirmação ou até mesmo vandalismo cibernético.

Entre todos os tipos de engenheiros sociais, os que mais preocupam são os pertencentes ao público interno, pois "[...] os ataques que vêm causando os maiores problemas para as organizações são aqueles que acontecem a partir da sua própria rede, ou seja, os ataques internos" (NAKAMURA E GEUS, 2007, p.28).

O público interno consiste em todas as pessoas que trabalham na OM, como os militares, funcionários civis e cessionários que prestam serviços no interior da OM. Essas pessoas têm uma vantagem muito importante que é a confiança daqueles que fazem parte da instituição. Além disso, conhecem a OM, seu organograma, a rotina, as instalações e detalhes específicos do serviço e das operações realizadas.

3.2.2 Meios e técnicas utilizadas

Os ataques de engenharia podem ser feitos por vários meios, entre eles o e-mail, o telefone, os CD/pendrives infectados com vírus e as redes sociais.

Entre as técnicas utilizadas estão: a observação, vasculhar o ambiente de trabalho, se passar por outras pessoas, usando a persuasão e realizar conversas aparentemente "inocentes" com militares das OM.

Muitas vezes uma ação de engenharia social é associada a outras técnicas para a obtenção de informação como, por exemplo, o trashing (revirar o lixo) e Captura de Informações Livre. Quando combinadas, essas técnicas podem causar problemas sérios às instituições atacadas, pois as informações obtidas por diferentes meios são cruzadas e dão origem a dados mais relevantes.

Independente do meio ou técnica utilizada, as principais características exploradas por um engenheiro social em relação ao fator humano são: reciprocidade, consistência, busca por aprovação social, simpatia, autoridade e medo (NAKAMURA E GEUS, 2007, p. 85). Ainda, segundo Assunção (2011, p.150) "os engenheiros sociais utilizam os sentimentos para manipulação e os casos mais comuns são: curiosidade, confiança, simpatia, culpa e medo".

3.2.2.1 E-mail

O e-mail é uma das ferramentas mais utilizadas por um engenheiro social devido à grande capilaridade que possui. As técnicas utilizadas para ataques por e-mail também podem ser aplicadas em outros meios como mensagens de telefone celular, aplicativos de relacionamento social e até mesmo correspondência física.

Uma técnica muito comum é a do e-mail com remetente falso, na qual o engenheiro social utiliza programas que podem gerar e-mails com endereço de remetentes que realmente existem, assim faz com que a vítima acredite que está recebendo uma mensagem de alguém confiável.

Outra técnica é a do e-mail manipulativo, em que a mensagem possui um conteúdo que pretende explorar a curiosidade ou ganância do militar. Normalmente, a mensagem trata de assuntos como "você ganhou 10 mil reais" ou "fotos comprometedoras que vazaram". O destinatário é levado a acessar os anexos, um link ou mandar informações para receber o tal prêmio e assim se torna mais uma vítima.

3.2.2.2 Hardware infectado

Ao aproveitar-se da confiança dos demais militares no ambiente de trabalho, um engenheiro social pode ter acesso a uma máquina e, por meio dos dispositivos ou de algum tipo de malware, conseguir extrair informações dos computadores e dos sistemas.

Também pode ser utilizado por engenheiros sociais externos às OM. Basta o atacante largar um hardware infectado em um local de

circulação dos militares da OM. Provavelmente este material será levado para a OM e infectará uma máquina.

3.2.2.3 Redes sociais

É por meio das redes sociais que um engenheiro social pode obter facilmente inúmeras informações sobre os militares, suas família e a OM.

A rede social pode ser utilizada para realizar ataques parecidos com os realizados por e-mails, com troca de mensagens em diálogos manipulativos que fazem com que a vítima forneça as informações desejadas; ou para a coleta de informações livres, onde o engenheiro social explora os perfis dos usuários em busca de informações como endereço, nomes, parentescos, profissão, local de trabalho, e-mail e telefone da vítima.

Além disso, criar um perfil falso em uma rede social como, por exemplo, o Facebook e o Whatsapp é muito fácil. Com algumas fotos já é possível criar um perfil e adicionar pessoas à sua conta. Assim, um engenheiro social pode se passar por um conhecido ou parente e solicitar informações que só seriam fornecidas a pessoas de confiança.

3.2.2.4 Telefone

O telefone é uma ferramenta muito utilizada. Com poucas informações o engenheiro consegue manter um diálogo que, por meio da manipulação dos sentimentos da vítima, o levará ao informe desejado. Não é uma técnica tão fácil, pois exige frieza e astúcia do engenheiro. Porém, quando bem utilizada, pode gerar vários problemas para uma instituição, sem oferecer grandes riscos ou gastos a quem realiza o ataque.

3.2.2.5 Ataques presenciais (personificação)

Um ataque clássico de engenharia social consiste em se fazer passar por um alto funcionário que tem problemas urgentes de acesso ao sistema. O hacker, assim, é como um ator, que, no papel que está representando, ataca o elo mais fraco da segurança de uma organização, que é o ser humano. (NAKAMURA E GEUS, 2007, p.85).

Acima temos um exemplo clássico de engenharia social, na qual um atacante se passa por um militar, conhecido/parente de algum militar, fornecedor, ou qualquer outro papel que lhe sirva. Deste modo, ele acaba obtendo acesso ao local ou consegue informações sobre a OM. A partir daí pode explorar o ambiente e outras vulnerabilidades.

3.2.2.6 Explorando o ambiente

Explorar o ambiente interno de uma OM é a única forma de obter informações que não se encontram disponíveis nos meios virtuais, como, por exemplo, plano de chamada. Outras informações podem ser obtidas ao se explorar o ambiente, como senha, logins e documentos deixados sobre as mesas de trabalho ou salvas nos computadores.

3.3 RISCOS ÀS OM E SEUS MILITARES

Uma vulnerabilidade presente nas OM é o fato de que grande parte dos militares oriundos do serviço militar obrigatório não tem nenhuma qualificação e possuem um baixo nível de escolaridade. Mesmo assim, muitos desses acabam trabalhando na operação de diversos sistemas dentro do quartel e têm acessos a diversas informações. Desconhecendo a importância que essas informações têm, eles podem se tornar vítimas ou deixar a instituição vulnerável.

Além disso, o compartilhamento dos computadores existentes, e o uso de equipamentos particulares, como pendrive e notebooks são práticas comuns, porque muitas OM sofrem com a falta desse tipo de material. Isso faz com que qualquer OM seja um alvo fácil para a instalação de vírus que pode comprometer os sistemas, extrair armazenar senhas e acessar bancos de dados.

Soma-se a tudo isso o fato de que o militar tende a confiar em todos aqueles que o cer-

cam no ambiente de trabalho. Porém, isso não é o ideal para uma instituição que pretende manter o ambiente de trabalho com boas práticas de segurança da informação, pois a confiança é um dos principais sentimentos explorados pelos engenheiros sociais.

4 MEDIDAS PREVENTIVAS

As medidas preventivas consideradas neste capítulo, compreendidas nos quadros de 1 a 5, têm como objetivo evitar os ataques de engenharia social contra as OM e seus militares.

QUADRO 1 - Ataques por e-mail (e similares)

TÉCNICA	MEDIDA PREVENTIVA
E-mail falso ou manipulativo	Desconfie sempre de mensagens de instituições financeiras, de ofertas imperdíveis, prêmios de promoções e mensagens com conteúdo do tipo "fotos comprometedoras".
	Evite fornecer informações sigilosas, mesmo para usuários de confiança.
	Mensagens de conhecidos nem sempre são confiáveis (o campo de remetente do e-mail pode ter sido falsificado, ou podem ter sido enviadas de contas falsas ou invadidas. (CERT.BR, 2017).
	Utilizar exclusivamente o correio eletrônico corporativo para troca de mensagens relativas ao serviço. (DCT, 2011).
	Não clicar em links ou abrir arquivos recebidos por e-mail, a menos que se tenha absoluta certeza da origem e integridade do mesmo. Ter em mente que um arquivo enviado por uma pessoa de confiança pode não ter sido realmente enviado por ela. (DCT, 2011).
	Não utilizar a conta de correio corporativo funcional em cadastros de sítios na Internet. Se necessário, manter uma conta em provedor público (Gmail, Yahoo, Hotmail, etc) para esta finalidade.

Fonte: AZZOLIN, 2017.

QUADRO 2 - Ataques por telefone (ou qualquer meio VoIP)

TÉCNICA	MEDIDAS PREVENTIVAS
Coleta de informações livres	Os atendes devem evitar se identificar de imediato ao atender a ligação.
Persuasão	Sempre confirmar a veracidade de informações recebidas
	Não fornecer/confirmar informações que não dizem respeito ao seu trabalho dentro da OM ou quando não se tem certeza de quem está do outro lado da linha.

Fonte: AZZOLIN, 2017.

QUADRO 3 - Redes Sociais

TÉCNICA	MEDIDAS PREVENTIVAS
Coleta de informações livres	Manter suas contas com configurações de privacidade mais restritas possíveis (evitar a configuração pública).
	Evitar expor informações pessoais como telefone, e-mail, endereço e até mesmo as relações familiares existentes com outros usuários.
	Desconfiar de perfis desconhecidos que solicitam permissão para se tornar "amigo" nas redes sociais.

TÉCNICA	MEDIDAS PREVENTIVAS
Persuasão	Evitar diálogos com perfis desconhecidos que exponham informações pessoais ou relacionadas com o trabalho em “chats” das diversas redes sociais existentes.
	Desconfie também de perfis de conhecidos solicitando informações (contas podem ser falsificadas facilmente).

Fonte: AZZOLIN, 2017.

QUADRO 4 - Ataques físicos

TÉCNICA	MEDIDAS PREVENTIVAS
Vasculhamento das instalações	Nunca deixar documentos sigilosos sobre as mesas ou de fácil acesso, assim como senha e login expostos.
	O controle de entrada e saída de pessoas pela guarda deve ser criterioso.
instalações	Pessoal externo à OM deve andar sempre acompanhado por um militar.
	Evite digitar senhas na presença de outras pessoas.
Persuasão	Exigir a apresentação do documento de identidade militar.
	Não forneça informações a recém conhecidos.
Acesso a máquinas/sistemas	Senhas e login de usuários não devem estar expostas.
	Evitar deixar senhas e login salvos nos navegadores, pois as senhas podem ser facilmente obtidas com recursos básicos de informática.
	Executar rigoroso controle das máquinas e dos usuários que podem ter acesso à rede de computadores da OM. Não permitir que máquinas de visitantes sejam conectadas à rede local. (DCT, 2011).
	Não possua senhas “universais” (iguais para todos os sistemas).
	Manter o sigilo das senhas utilizadas nos sistemas computacionais. As senhas são pessoais, não podendo, portanto, ser compartilhadas. (DCT, 2011).
	Os cadastros de usuários que acessam os sistemas devem ser mantidos atualizados e supervisionados pela contrainteligência da OM. (DCT, 2011).
	Estabelecer uma política clara e supervisionada relativa ao descredenciamento de usuários que tenham sido transferidos de OM ou de função. (DCT, 2011).
Vasculhamento do lixo	Não jogue fora documentos com informações sigilosas. Separe e elimine de forma eficiente.

Fonte: AZZOLIN, 2017.

QUADRO 5 - Controle de Hardwares

TÉCNICA	MEDIDAS PREVENTIVAS
Instalação de vírus por meio de hardwares infectados	Proibir a utilização de dispositivos móveis de armazenamento (pendrives, HD externos ou cartões de memória), particularmente em ambientes onde operam máquinas com dados sensíveis. Quando absolutamente necessário, liberar o acesso de tais dispositivos, sob supervisão. (DCT, 2011).
	Configurar o antivírus para verificar automaticamente todos os dispositivos de armazenamento removíveis (CD, DVD, pendrive, cartão de memória, HD externo etc.) conectados ao computador. (DCT, 2011).

Fonte: AZZOLIN, 2017.

É importante que haja em cada OM uma política para a restrição de circulação dos próprios militares dentro das repartições administrativas. Acreditar que o ambiente militar é sempre seguro e confiável é um dos erros mais cometidos por possíveis vítimas.

Todos os ataques e situações suspeitas

devem ser reportados à Seção de Inteligência da OM, para que seja repassado aos militares interessados e ao pessoal de serviço, a fim de evitar outros ataques.

5 CONCLUSÃO

As medidas preventivas apresentadas nessa pesquisa científica têm como objetivo evitar que militares e instituições do EB sofram danos causados por ações de engenharia social. Dessa forma, essa pesquisa visa ajudar na confecção de uma PSI quando o assunto considerado for a engenharia social.

Porém, essas medidas são apenas uma parte do que deve haver em uma PSI, pois ela abrange muitos outros aspectos de segurança da informação relacionados à cibernética, instalações físicas e gestão de recursos humanos.

Essa correta gestão da segurança da informação pode mitigar a prática de crimes cibernéticos preservando a segurança orgânica da OM e a integridade dos militares, melhorando a imagem e credibilidade das instituições.

Isso cresce de importância, à medida que os crimes cibernéticos estão se tornando cada vez mais comuns. Tanto contra instituições, quanto contra pessoas. Por isso, as:

> [...] políticas de segurança das informações não podem ser inflexíveis. Uma empresa precisa mudar à medida que surgem novas tecnologias de segurança, e à medida que as vulnerabilidades de segurança evoluem, as políticas precisam ser modificadas ou suplementadas (FONSECA, 2009, p. 06).

Portanto, o assunto não se esgota aqui. É necessário sempre atualizar a PSI e as medidas preventivas quanto aos novos tipos e ataques e ameaças que surgirem.

Em relação à segurança do aquartelamento é possível considerar que “seria um grande erro focar só no lado físico da coisa, o treinamento dos empregados é essencial” (ASSUNÇÃO, 2011, p. 164). Portanto, instruções com a finalidade de apresentar os novos tipos de ataques aos militares da OM devem ocorrer com frequência.

Todas as pessoas de uma empresa que lidam com informações importantes devem passar por um treinamento no qual irão aprender a identificar os tipos de ataque e como reagir a cada um deles (ASSUNÇÃO, 2011, p. 164). Isso deve ocorrer sempre que alguém assumir uma função que demanda maior cuidado com as informações.

Porém, a simples realização de um programa de conscientização não é o suficiente. É necessário que haja fiscalização em todos os níveis e de todos os procedimentos. Os militares devem ser alertados dos perigos constantemente e corrigidos (inclusive dentro do aspecto disciplinar) ao executarem algum procedimento incorreto. Para a fiscalização, podemos considerar o seguinte:

> [...] testes periódicos de penetração e avaliações de vulnerabilidade que usamos métodos e as táticas da engenharia social devem ser conduzidos para expor os pontos fracos do treinamento ou a falta de cumprimento das políticas e dos procedimentos da empresa (FONSECA, 2009, p. 06).

Diante de tudo que foi apresentado, é inegável que a defesa cibernética, seja ela no nível tático ou estratégico, merece cada vez mais atenção dos órgãos e competentes, assim como do comando de cada OM.

É imperativo que, em todos os níveis, exista conscientização e preparo para agir perante os mais diversos tipos de ataque, negando sempre que possível, a obtenção de informações por organizações criminosas ou pessoas isoladas. Tudo isso para que o EB possa dar continuidade ao seu trabalho como Instituição permanente das Forças Armadas.

SOCIAL ENGINEERING ATTACKS: PREVENTIVE MEASURES FOR INFORMATION SECURITY

ABSTRACT. The present scientific research has as its theme the social engineering attacks

on the OM and its military. The aim of the work is to raise the preventive measures (to elaborate an information security policy) capable of avoiding social engineering attacks against the Brazilian Army Organizations and the military that serve them. In order to be able to raise such preventive measures, a bibliographical research was carried out about the social engineering threats and main vulnerabilities of OM. A study on information security policy was also necessary, in order to select better actions, guidelines and standards capable of avoiding attacks of this nature. As a result, the scientific work shows what preventive measures should be considered for the correct safety of the information asset in relation to social engineering. Finally, the research explains how these measures should be approached for the better awareness of the internal public and presents other characteristics indispensable to an information security policy, so that it fulfills its purpose. The content presented makes the research relevant by helping to synthesize preventive measures of social engineering attacks directed specifically to the military environment and to collaborate in this way to improve the policies of military awareness and protection of information.

Keywords: Precautionary Measures. Social Engineering. Information Security Policy.

REFERÊNCIAS

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do Hacker Ético**. 4. ed. Florianópolis: Visual Books, 2011.

BRASIL. Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações. 1. Ed. 09f. [S.l.]: Departamento de Ciência e Tecnologia, 2011.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Cartilha de segurança para internet. [S.l.]: 2017. Disponível em: <https://cartilha.cert.br/golpes/>. Acesso em: 15 maio 2017.

CRESPO, Marcelo Xavier De Freitas. **Crimes Digitais**. 1. ed. São Paulo: Saraiva, 2011.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação**: O Fator Humano. 16f. Artigo Científico. Curitiba: Pontifícia Universidade Católica do Paraná, 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf>. Acesso em: 15 maio 2017.

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

MANDARINO, Raphael. **Um estudo sobre a segurança do espaço cibernético brasileiro**. Brasília: Cubzac, 2009.

MICHAELIS. **Significado da palavra cibernética**. [S.l.]: 2017. Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=cibernetica>. Acesso em: 18 maio 2017.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Licio. **Segurança de redes em ambientes cooperativos**. 1. ed. São Paulo: Novatec, 2007.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras - AMAN, pós-graduado, Lato Sensu, em em Oficial de Comunicações pela EsCom e pode ser contactado pelo e-mail matheusmurari@hotmail.com.