Gestão de Segurança da Informação: O Fator Humano

Paula Fernanda Fonseca

Curso de Pós Graduação em Redes e Segurança de Computadores da Pontifícia Universidade Católica do Paraná

Curitiba, Novembro de 2009.

Resumo

Apesar do aumento da preocupação das organizações com a proteção e a segurança da informação e dos grandes investimentos em mecanismos modernos para o controle de informações, essas ações, isoladamente, podem não ser eficazes. Em conjunto com essas medidas, deve ser implantado um Programa de Segurança da Informação, capaz de instruir e conscientizar toda a equipe de trabalhadores da organização sobre a importância das informações manipuladas e do papel de cada um com a segurança dessas informações. Nesse Programa deve ser incluída a constante disseminação do assunto entre todos e a elaboração de Políticas Internas que demonstrem a conduta esperada pela Organização em relação aos cuidados com a informação e às medidas mais adequadas para sua proteção e abordem, também, um rol de conseqüências quando da inobservância das medidas recomendadas.

1. Introdução

As organizações estão cada vez mais expostas as ameaças que surgem sobre o seu principal ativo: a informação. Investimentos são feitos em segurança física (CFTV, controle de acesso, alarmes) e lógica (antivirus, softwares de detecção de intrusão) para dificultar o acesso não autorizado aos ambientes de armazenamento e processamento das informações. Contudo, se seus principais conhecedores e manipuladores (colaboradores) não estiverem capacitados, treinados e conscientizados sobre seu papel no processo de proteção das informações da organização todo esse investimento não será justificado.

É principalmente sobre o fator humano que ocorre grande parte dos vazamentos de informações, seja por descontentamento do colaborador com a organização, o qual pode não se sentir valorizado ou por técnicas de Engenharia Social.

Para se minimizar essa exposição as organizações precisam adotar políticas de segurança da informação, normas e procedimentos claros que sejam constantemente atualizadas e disseminadas a todos os seus colaboradores através de programas e treinamentos de conscientização.

1.1 Estrutura do Artigo

Na primeira parte do artigo será feita uma abordagem sobre o problema: segurança da informação x fator humano descrevendo um dos maiores, se não o principal, problema enfrentado pelo elo mais fraco da segurança a Engenharia Social. Em seguida, é possível visualizar sugestões de soluções para esse problema seguido de uma análise comparativa entre problemas x soluções. E a última etapa é feita uma conclusão sobre o assunto.

2. Descrição detalhada do problema

"Segurança tem início e termina nas pessoas."
Ellen Frisch

As organizações estão cada vez mais expostas aos riscos causados pelo vazamento de suas informações. Esse vazamento poderá ser dado através de uma invasão física, lógica ou humana. A preservação da confidencialidade dessas informações é de responsabilidade de todos os colaboradores, que na maioria das vezes não estão preparados para lidar e reconhecer situações de riscos. Por exemplo, um colaborador insatisfeito pode revelar segredos estratégicos que causem impactos a imagem da empresa e/ou perdas financeiras.

Um dos grandes problemas, se não o maior, com relação a Segurança da Informação do ponto de vista humano é uma técnica chamada de Engenharia Social, pois através dela o engenheiro social utiliza diversos métodos para obter acesso as informações confidenciais das empresas.

2.1 Engenharia Social

"É a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos" [3].

Os ataques de Engenharia Social podem ser realizados através de algumas ferramentas, são elas:

- ✓ **Telefone ou VolP (voz sobre IP)** - passar-se por alguém que não é seria um dos típicos ataques de engenharia social, como na personificação - help-desk;
- ✓ **Internet (coleta de informações)** - como, por exemplo, sites que fornecem id;
- ✓ **Intranet (acesso remoto)** - 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 scam);*
- ✓ **Pessoalmente (In Person Social Engineering) -** poder de persuasão, habilidade em saber conversar, tipo de ataque mais raro.
- ✓ **Chats** (bate papo) - Fazer-se passar por alguém que na verdade não é fica muito mais fácil pelos canais de bate-papo.
- ✓ **Fax** - Primeiramente, obter o número do fax da pessoa física ou jurídica para que se possa começar o ataque.
- ✓ **Cartas/correspondência** - Não é o meio mais moderno sem dúvida, mas, acredite, é um recurso poderoso que faz como uma das maiores vítimas as pessoas mais velhas.
- ✓ **Spyware** - Software "espião" usado para monitorar de modo o-culto as atividades do computador de um alvo;
- ✓ **Mergulho no lixo ("Dumpster diving") -** Várias coisas que são descartadas para o lixo muitas vezes contêm informações essenciais ao suposto engenheiro social;
- ✓ **Surfar sobre os ombros** - É o ato de observar uma pessoa digitando no teclado do computador para descobrir e roubar sua senha ou outras informações de usuário.

- ✓ **P2P (Peer-to-Peer)** - Tecnologia empregada para estabelecer comunicação entre inúmeros computadores, como uma rede, onde cada estação possui capacidades e responsabilidades equivalentes. [3]

Para que seja possível usá-las o Engenheiro Social utiliza técnicas relativamente simples e clássicas, como por exemplo, pedindo a informação ou oferecendo ajuda à suposta vítima.

3. Descrição das soluções disponíveis

Os colaboradores devem ser treinados e educados sobre quais são as informações que devem ser protegidas e como devem protegê-la, pois com isso estarão aptos a identificar situações de riscos, como um ataque de Engenharia Social.

Para criar e disseminar essa consciência as organizações devem criar e divulgar suas políticas, normas e procedimentos de segurança da informação através de programas de treinamento e conscientização constantes.

3.1 O que é uma Política de Segurança da Informação?

As políticas de segurança são instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações, e é um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança. Essas políticas estão entre as mais significativas no que diz respeito a evitar e detectar os ataques da engenharia social.

Os controles efetivos de segurança são implementados pelo treinamento dos empregados, bem como por políticas e procedimentos bem documentados. Entretanto, é importante observar que as políticas de segurança, mesmo que sejam seguidas religiosamente por todos os empregados, não evitam todos os ataques da engenharia social. Por isso, um objetivo ideal seria sempre minimizar o risco até um nível aceitável.

As políticas apresentadas aqui incluem medidas que, embora não se concentrem estritamente nas questões da engenharia social, estão aqui porque tratam das técnicas normalmente usadas nos ataques da engenharia social. Por exemplo, as políticas sobre a abertura dos anexos de correio eletrônico - as quais podem instalar software Cavalo de Tróia, permitindo que o atacante tome o computador da vítima — abordam um método muito usado pêlos invasores de computadores.

Um programa de segurança da informação abrangente começa com uma avaliação de risco que visa determinar:

- ✓ Quais são as informações da empresa que precisam ser protegidas?
- ✓ Quais ameaças específicas existem contra os ativos?
- ✓ Qual dano seria causado às empresas se essas ameaças em potencial se materializassem?

O objetivo primário da avaliação de risco é priorizar as informações que precisam de proteção imediata, e se essa proteção será eficaz em termos de custo com base em uma análise do custo/benefício. Em resumo, quais informações serão protegidas em primeiro lugar e quanto custará para proteger essas informações?

É essencial que a gerência de primeiro escalão adote e suporte com firmeza o desenvolvimento de políticas de segurança e de um programa de segurança das informações. Assim como qualquer ou método corporativo, para que um programa de segurança seja bem-sucedido, a gerência deve fazer mais do que apenas apoiá-lo, deve demonstrar um comprometimento pelo exemplo pessoal. Os empregados precisam ter consciência de que a gerência acredita que a segurança das informações é' para a operação da empresa, de que a proteção das informações comerciais da empresa é essencial para que ela continue funcionando e de que o trabalho de cada empregado pode depender do sucesso do programa.

A pessoa designada para criar as políticas de segurança da informação precisa entender que as políticas devem ser escritas em um estilo que não faça uso de jargão técnico e que possa ser facilmente entendido pelo empregado não técnico. Também é importante que o documento deixe claro que cada política é importante, caso contrário os empregados podem encará-las como perda de tempo e não cumpri-las. O redator dessa política deve criar um documento que apresente as políticas e um documento separado para os procedimentos, porque as políticas provavelmente mudam com menos freqüência do que os procedimentos específicos usados para implementá-las.

Além disso, o redator das políticas deve estar consciente dos meios pêlos quais as tecnologias da segurança podem ser usadas para implantar as boas práticas da segurança das informações. Por exemplo, a maioria dos sistemas operacionais possibilita a solicitação de que as senhas de usuário atendam a determinadas especificações, tais como tamanho. Em algumas empresas, uma política que proíbe que os usuários façam o download de programas pode ser controlada por meio de definições locais ou globais de diretrizes de segurança dentro do sistema operacional. As políticas devem exigir o uso da tecnologia sempre que isso for eficaz em termos de custo, para remover a tomada de decisão com base nas pessoas.

Os empregados devem ser aconselhados sobre as conseqüências do não-cumprimento das políticas e dos procedimentos de segurança. Um resumo das conseqüências da violação das políticas deve ser desenvolvido e amplamente divulgado. Por sua vez, um programa de recompensa deve ser criado para os empregados que demonstram boas práticas de segurança ou que reconhecem e relatam um incidente de segurança. Sempre que um empregado for recompensado por frustrar uma quebra de segurança, isso deve ser amplamente divulgado em toda a empresa, como por exemplo, em um artigo na circular da empresa.

Um dos objetivos de um programa de conscientização sobre a segurança é a comunicação da importância das políticas de segurança e o dano que a falha em seguir essas regras pode causar. Dada à natureza humana, os empregados às vezes ignoram ou sabotam as políticas que parecem ser injustificadas ou que demandam muito tempo. A gerência tem a responsabilidade de garantir que os empregados entendam a importância das políticas e sejam motivados para atendê-las, e não tratá-las como obstáculos a serem contornados.

E importante notar que 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. Um processo de exame e atualização regular deve ser estabelecido. Torne as políticas e os procedimentos de segurança corporativa disponível por meio da intranet corporativa ou mantenha-os em uma pasta que esteja disponível para todos. Isso aumenta a probabilidade de que tais políticas e procedimentos sejam examinados com mais freqüência e fornece um método conveniente para que os empregados encontrem rapidamente a resposta para todas as perguntas relacionadas com a segurança das informações.

Finalmente, testes periódicos de penetração e avaliações de vulnerabilidade que usam os 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. Antes de usar qualquer tática de teste de penetração simulado, os empregados devem ser avisados de que tais testes podem ocorrer de tempos em tempos.

As políticas detalhadas apresentadas neste capítulo representam apenas um subconjunto das políticas de segurança das informações que, creio, sejam necessárias para diminuir todos os riscos de segurança. Da mesma forma, as que estão incluídas aqui não devem ser consideradas como uma lista abrangente de políticas de segurança das informações. Em vez disso, elas formam a base para a criação de um corpo abrangente de políticas de segurança que sejam apropriadas para as necessidades específicas da sua empresa.

Os redatores das políticas de uma organização terão de escolher as políticas apropriadas com base no ambiente e nos objetivos de negócios de suas empresas. Cada organização, com seus requisitos de segurança diferentes, baseados nas necessidades, nos requisitos legais, na cultura organizacional e nos sistemas de informações utilizados estabelecerão as políticas apresentadas e omitirá restante.

Também é preciso fazer opções sobre a rigidez das políticas em cada categoria. Uma empresa menor localizada em uma única instalação na qual a maioria dos empregados se conhece não precisa estar muito preocupada com o fato de o atacante ligar e se fazer passar por um empregado (embora, é claro, um impostor pode se fazer passar por um fornecedor). Da mesma forma, apesar dos riscos maiores, uma empresa estruturada com uma cultura corporativa mais liberal e solta pode querer adotar apenas um subconjunto limitado das políticas recomendadas para atender a seus objetivos de segurança. [2]

3.2 Criando programas de treinamento e conscientização

Importante conscientizar as pessoas sobre o valor da informação que elas dispõem e manipulam, seja ela de uso pessoal ou institucional. Informar os usuários sobre como age um engenheiro social.

O seu risco não diminui com o simples fato de você criar um panfleto sobre a política de segurança ou enviar seus empregados para uma página da intranet que detalha as políticas de segurança. As empresas devem não apenas definir por escrito as regras das políticas, mas também devem se esforçar ao máximo para orientar todos os que trabalham com as informações corporativas ou com os sistemas de computadores para que eles aprendam e sigam as regras. Além disso, você deve garantir que todos entendam o motivo de cada política, para que as pessoas não tentem se desviar da regra por questões de conveniência. Caso contrário, a ignorância sempre será a melhor desculpa do empregado, e é exatamente essa vulnerabilidade que os engenheiros sociais vão explorar.

O objetivo central de um programa de conscientização sobre segurança é influenciar as pessoas para que elas mudem seu comportamento e suas atitudes motivando cada empregado a querer entrar no programa e fazer a sua parte para proteger os ativos de informações da organização. Um ótimo motivador nesse caso é explicar como a participação das pessoas beneficiará não apenas a empresa, mas também os empregados individuais. Como a empresa detém determinadas informações particulares sobre cada funcionário, quando os

empregados fazem a sua parte para proteger as informações ou os sistemas de informações, na verdade eles estão protegendo também as suas próprias informações.

Um programa de treinamento em segurança requer um suporte substancial. O esforço de treinamento precisa atingir cada pessoa que tem acesso a informações confidenciais ou aos sistemas corporativos de computadores, deve ser contínuo e ser sempre revisado para atualizar o pessoal sobre as novas ameaças e vulnerabilidades. Os empregados devem ver que a direção está totalmente comprometida com o programa. Esse comprometimento deve ser real, e não apenas um memorando com um carimbo que diz "Nós dizemos amém". E o programa deve ser fundamentado por recursos suficientes para desenvolver, comunicar, testar e medir o sucesso.

A orientação básica que deve ser lembrada durante o desenvolvimento de um programa de treinamento e conscientização em segurança é que o programa precisa se concentrar em criar em todos os empregados à consciência de que a sua empresa pode ser atacada a qualquer momento. Eles devem aprender que cada empregado tem um papel na defesa contra qualquer tentativa de entrar nos sistemas de computadores ou de roubar dados confidenciais.

Como muitos aspectos da segurança das informações envolvem a tecnologia, é muito fácil para os empregados acharem que o problema está sendo tratado por *firewalls* e por outras tecnologias de segurança. Um dos objetivos principais do treinamento deve ser a criação em cada empregado da consciência de que eles são a linha de frente necessária para proteger a segurança geral da organização.

O treinamento em segurança deve ter um objetivo significativamente maior do que simplesmente impor regras. O criador do programa de treinamento deve reconhecer a forte tentação dos empregados sob pressão de fazer seus trabalhos e de ignorar suas responsabilidades de segurança. O conhecimento das táticas da engenharia social e de como se defender dos ataques é importante, mas não servirá para nada se o treinamento não se concentrar bastante na motivação dos empregados para que usem o conhecimento.

A empresa pode considerar que o programa está atingindo o seu objetivo final se todos os que realizarem o treinamento estiverem convencidos e motivados por uma noção básica: a noção de que a segurança das informações faz parte do seu trabalho.

Os empregados devem refletir e aceitar que a ameaça dos ataques da engenharia social é real e que uma perda de informações confidenciais da empresa pode ameaçar a empresa e também as suas informações pessoais e os seus empregos. De certa forma, não cuidar da segurança das informações no trabalho é o mesmo que não cuidar do cartão de

banco ou do número do cartão de crédito de alguém. Essa pode ser uma analogia convincente para criar o entusiasmo pelas práticas de segurança.

A pessoa responsável pela criação do programa de segurança das informações precisa reconhecer que esse não é um projeto de "tamanho único". Pelo contrário, o treinamento precisa ser desenvolvido para se adequar aos requisitos específicos de diversos grupos dentro da empresa. Embora muitas das políticas de segurança destacadas no Capítulo 16 apliquem-se a todos os empregados da empresa, muitas outras são exclusivas. No mínimo, a maioria das empresas precisará de programas de treinamento adaptados a esses grupos distintos: os gerentes, o pessoal de TI, os usuários de computadores. O pessoal das áreas não técnicas, os assistentes administrativos, os recepcionistas e o pessoal de segurança.

Como o pessoal da segurança de uma empresa normalmente não deve ser proficiente em computadores, e, exceto talvez de uma forma muito limitada não entre em contato com os computadores da empresa, eles geralmente não são considerados quando da criação de treinamentos desse tipo. Entretanto, os engenheiros sociais podem enganar os guardas de segurança ou outros para que eles lhes permitam a entrada em um prédio ou escritório, ou para que executem uma ação que resulte em uma invasão de computador. Embora os membros da segurança certamente não precisem do mesmo treinamento completo pelo qual passam as pessoas que operam ou usam os computadores, eles não devem ser esquecidos no programa de conscientização sobre a segurança.

Dentro do mundo corporativo talvez haja poucos assuntos sobre os quais todos os empregados precisam ser treinados e que são ao mesmo tempo tão importantes e tão aborrecidos quanto a segurança. Os melhores programas de treinamento sobre a segurança das informações devem informar e prender a atenção e o entusiasmo dos aprendizes.

O objetivo deve transformar a conscientização e o treinamento em segurança das informações em uma experiência interessante e interativa. As técnicas podem incluir a demonstração dos métodos da engenharia social por meio da dramatização, o exame de relatórios da mídia sobre ataques recentes em outras empresas com menos sorte e a discussão das maneiras pelas quais as empresas poderiam ter evitado o prejuízo. Elas também podem mostrar um vídeo sobre segurança que seja divertido e educacional ao mesmo tempo. Existem diversas empresas de conscientização sobre a segurança que comercializam vídeos e materiais relacionados.

As histórias deste livro fornecem um material rico para explicar os métodos e as táticas da engenharia social e têm o objetivo de aumentar a consciência sobre a ameaça e de demonstrar as vulnerabilidades do comportamento humano. Pense em usar os cenários aqui

descritos como a base para as atividades de dramatização. As histórias também oferecem oportunidades para discussões animadas sobre como as vítimas poderiam ter respondido de forma diferente para evitar que os ataques fossem bem-sucedidos.

Um desenvolvedor habilidoso de cursos e treinadores habilidosos encontrarão muitos desafios, mas também muitas oportunidades para manter a classe interessada e, ao mesmo tempo, para motivar as pessoas a tomarem parte na solução.

Um programa básico de treinamento na conscientização sobre segurança deve ser desenvolvido de modo que todos os empregados tenham de participar. Os empregados novos devem participar dele, como parte de seu treinamento inicial. Recomendo que nenhum empregado receba acesso a um computador antes de ter participado de uma sessão básica de conscientização sobre a segurança.

Para essa etapa inicial, sugiro uma sessão que seja voltada para prender a atenção e que seja curta o suficiente para que as mensagens importantes sejam lembradas. Embora a quantidade do material abordado justifique um treinamento mais longo, a importância de fornecer a conscientização e a motivação juntamente com um número razoável de mensagens essenciais, a meu ver, é mais eficiente do que longas sessões de meio dia ou dia inteiro que deixam as pessoas tontas com tantas informações.

A ênfase dessas sessões deve estar na veiculação de uma apreciação sobre o mal que pode ser feito à empresa e aos empregados, a menos que todos tenham bons hábitos de segurança no trabalho. Mais importante do que aprender sobre as práticas específicas de segurança é a motivação que leva os empregados a aceitarem a responsabilidade pessoal pela segurança.

Em situações nas quais alguns empregados não podem participar das sessões em classe, a empresa deve pensar em desenvolver o treinamento em conscientização usando outras formas de instrução, tais como vídeos, treinamento baseado em computador, cursos on-line ou material escrito.

Após a sessão de treinamento inicial, sessões mais longas devem ser criadas para educar os empregados sobre as vulnerabilidades específicas e técnicas de ataque relativas à sua posição na empresa. Pelo menos uma vez por ano é preciso fazer um treinamento de renovação. A natureza da ameaça e os métodos usados para explorar as pessoas estão sempre mudando, de modo que o conteúdo do programa deve ser mantido atualizado. Além disso, a consciência e o preparo das pessoas diminui com o tempo, de modo que o treinamento deve se repetir a intervalos razoáveis de tempo para reforçar os princípios da segurança. Novamente a ênfase precisa estar em manter os empregados convencidos sobre a importância

das políticas de segurança e motivados para que as sigam, além de expor as ameaças específicas e os métodos da engenharia social.

Os gerentes devem dar um tempo razoável a seus subordinados para que eles se familiarizem com as políticas e os procedimentos de segurança e para que participem do programa de conscientização sobre a segurança. Não se deve esperar que os empregados estudem as políticas de segurança nem participem das aulas no seu tempo vago. Os empregados novos devem ter um tempo maior para examinar as políticas de segurança e as práticas estabelecidas antes de iniciar as responsabilidades da sua função.

Os empregados que mudarem de posição dentro da organização para uma função que envolva o acesso a informações confidenciais ou sistemas de computadores devem, obviamente, fazer um programa de treinamento em segurança adaptado às suas novas responsabilidades. Por exemplo, quando um operador de computador torna-se um administrador de sistema ou quando uma recepcionista torna-se uma assistente administrativa, ambos devem passar por um novo treinamento.

Quando reduzidos às suas características fundamentais, todos os ataques da engenharia social têm o mesmo elemento comum: a fraude. A vítima é levada a acreditar que o atacante é um colega ou alguma outra pessoa que está autorizada a acessar informações confidenciais ou que está autorizada a dar à vítima instruções que envolvam a tomada de ações com um computador ou com equipamento relacionado com o computador. Quase todos esses ataques poderiam ser evitados se o empregado alvo seguisse estas etapas:

- ✓ Verificar a identidade da pessoa que faz a solicitação: essa pessoa é realmente quem diz ser?
- ✓ Verificar se a pessoa está autorizada. A pessoa tem a necessidade de saber ou tem autorização para fazer a solicitação?

Se as sessões de treinamento de conscientização puderem mudar o comportamento das pessoas para que cada empregado sempre teste toda solicitação que contraria esses critérios, o risco associado aos ataques da engenharia social reduzir-se-á de modo impressionante.

Um programa prático de treinamento e conscientização sobre a segurança das informações que aborda os aspectos do comportamento humano e da engenharia social deve incluir:

- ✓ Uma descrição do modo como os atacantes usam as habilidades da engenharia social para enganar as pessoas.
- ✓ Os métodos usados pêlos engenheiros sociais para atingir seus objetivos.

- ✓ Como reconhecer um provável ataque da engenharia social
- ✓ O procedimento para o tratamento de uma solicitação suspeita.
- ✓ A quem relatar as tentativas da engenharia social ou os ataques bem-sucedidos.
- ✓ A importância de questionar todos os que fazem uma solicitação suspeita, independentemente da posição ou importância que a pessoa alega ter.
- ✓ O fato de que os funcionários não devem confiar implicitamente nas outras pessoas sem uma verificação adequada, embora o seu impulso seja dar aos outros o benefício da dúvida.
- ✓ A importância de verificar a identidade e a autoridade de qualquer pessoa que faça uma solicitação de informações ou ação. (Consulte "Procedimentos de verificação e autorização" no Capítulo 16 para obter detalhes sobre como verificar a identidade.)
- ✓ Procedimentos para proteger as informações confidenciais, entre eles a familiaridade com todo o sistema de classificação de dados.
- ✓ A localização das políticas e dos procedimentos de segurança da empresa e a sua importância para a proteção das informações e dos sistemas de informações corporativas.
- ✓ Um resumo das principais políticas de segurança e uma explicação do seu significado. Por exemplo, cada empregado deve ser instruído sobre como criar uma senha difícil de adivinhar.
- ✓ A obrigação de cada empregado de atender às políticas e as conseqüências do seu não-atendimento.

Por definição, a engenharia social envolve algum tipo de interação humana. Com frequência, um atacante usa vários métodos de comunicação e tecnologias para tentar atingir o seu objetivo. Por esse motivo, um programa de conscientização bem feito deve tentar abordar alguns ou todos estes itens:

As políticas de segurança relacionadas com senhas de computador e *voice mail*.

- ✓ O procedimento de divulgação de informações ou material confidencial.
- ✓ A política de uso do correio eletrônico, incluindo as medidas para evitar ataques maliciosos de código, tais com vírus, *worms* e Cavalos de Tróia.
- ✓ Os requisitos de segurança física, tais como o uso de crachás.
- ✓ A responsabilidade de questionar as pessoas que estão nas instalações sem o crachá.
- ✓ As melhores práticas de segurança para o uso do *voice mail.*

- ✓ Como determinar a classificação das informações e as medidas adequadas para proteger as informações confidenciais.
- ✓ A eliminação adequada de documentos confidenciais e mídia de computador que contenham, ou que já tenham contido material confidencial.

Da mesma forma, se a empresa pretende usar testes para determinar a eficiência das defesas contra os ataques da engenharia social, um aviso deve ser dado para que os empregados tomem conhecimento dessa prática. Deixe que saibam que em algum momento eles podem receber uma ligação telefônica ou outra comunicação que usará as técnicas do atacante como parte de tal teste. Use os resultados desses testes não para punir, mas para definir a necessidade de treinamento adicional em algumas áreas.

A maioria das pessoas sabe que o aprendizado, mesmo das questões importantes, tende a desaparecer, a menos que seja reforçado periodicamente. Devido à importância de manter os empregados atualizados sobre o assunto da defesa contra os ataques da engenharia social, um programa constante de conscientização é de importância vital.

Um método para manter a segurança sempre na mente do empregado é fazer com que a segurança das informações seja parte específica da função de todas as pessoas que trabalham na empresa. Isso as encoraja a reconhecer o seu papel crucial na segurança geral da empresa. Caso contrário há uma forte tendência de achar que a segurança "não é problema meu".

Embora a responsabilidade geral por um programa de segurança das informações normalmente seja de uma pessoa do departamento de segurança ou do departamento de tecnologia da informação, o desenvolvimento de um programa de conscientização para a segurança das informações provavelmente é mais bem estruturado como um projeto conjunto com o Departamento de Recursos Humanos.

O programa constante de conscientização precisa ser criativo e usar cada canal disponível para comunicar as mensagens de segurança para que elas sejam lembradas e para que os empregados tenham sempre em mente os bons hábitos de segurança. Os métodos devem usar todos os canais tradicionais, além dos não tradicionais que sejam imaginados pelas pessoas designadas para implementar e desenvolver o programa. Assim como acontece na propaganda tradicional, o humor e a inteligência ajudam. A mudança na redação das mensagens evita que elas se tornem familiar demais para serem ignoradas.

A lista de possibilidades de um programa constante de conscientização poderia incluir:

- ✓ O fornecimento de exemplares deste livro para todos os empregados.

- ✓ A inclusão de itens informativos nas circulares da empresa: por exemplo, artigos, lembretes (de preferência itens curtos que chamem a atenção) ou quadrinhos.
- ✓ A colocação de uma foto do Empregado da Segurança do Mês.
- ✓ Pôsteres afixados nas áreas dos empregados.
- ✓ Notas publicadas no quadro de avisos.
- ✓ O fornecimento de lembretes impressos nos envelopes de pagamento.
- ✓ O envio de lembretes por correio eletrônico.
- ✓ O uso de proteções de tela relacionadas com segurança.
- ✓ A transmissão de anúncios sobre a segurança por meio do sistema de *voice mail*.
- ✓ A impressão de etiquetas para o telefone com mensagens tais como "A pessoa que está ligando é quem ela diz ser?".
- ✓ A configuração de mensagens de lembrete que aparecem quando o computador é ligado, tais como "Criptografe as informações confidenciais antes de enviá-las".
- ✓ A inclusão da conscientização para a segurança como um item-padrão nos relatórios de desempenho dos empregados e nas análises anuais.
- ✓ A publicação na intranet de lembretes de conscientização para a segurança, talvez usando quadrinhos ou humor, ou alguma outra maneira que incentive as pessoas a lerem.
- ✓ O uso de um quadro eletrônico de mensagens na lanchonete, com um lembrete de segurança que seja trocado frequentemente.
- ✓ A distribuição de folhetos ou brochuras. E pense naqueles biscoitos da fortuna que são distribuídos de graça na lanchonete, contendo cada um deles um lembrete sobre a segurança em vez de uma previsão. A ameaça é constante; os lembretes também devem ser constantes. [2]

4. Análise comparativa

Para conseguir minimizar os riscos de vazamento das informações confidenciais, as quais poderão acarretar algum tipo de prejuízo seja a imagem da instituição, ao seu patrimônio ou financeiro, as organizações devem criar procedimentos claros para todos os processos onde essas informações circulem.

A seguir serão listados alguns riscos que as organizações estão expostas devido à falta de treinamento e conscientização dos seus colaboradores.

- ✓ **Acesso indevido aos ambientes da empresa** – as organizações devem adotar procedimentos que permitam a seus colaboradores reconhecer se uma determinada pessoa é realmente quem diz ser. Pois caso contrário, pessoas mal intencionadas podem conseguir, através de uma das técnicas utilizadas pela Engenharia Social ludibriá-las e terem acesso aos ambientes da organização. Para isso as organizações devem investir em mecanismos que possibilitem a identificação de visitantes, prestadores de serviços e seus colaboradores.
- ✓ **Fornecimento de senha de acesso aos sistemas da empresa** – em um simples telefonema um Engenheiro Social pode conseguir obter a senha de um colaborador da organização que o permitirá ter acesso aos sistemas internos da organização sem maiores problemas. Para que isso não ocorra o colaborador deve ser treinado sobre quais são as informações que podem ser de acesso público e privado essa conscientização deve ser feita através da criação e divulgação de normas de procedimentos que digam a ele qual é a postura que deve ser tomada diante de situações que possam representar risco para a organização.
- ✓ **Descarte físico das informações** – de nada adiantará a organização ter mecanismos modernos de controle de acesso as informações lógicas se não houver procedimentos que digam aos colaboradores que o descarte das informações físicas deve ser realizado através de meios seguros como por exemplo, fragmentadoras. Informações importantes relativas ao negócio da empresa, projetos internos e de clientes podem ser encontradas no lixo por pessoas que pretendem de alguma forma utilizá-las para benefício próprio.

5. Conclusão

A informação está exposta a diversos tipos de ataques, seja através de meios físicos, lógicos ou humanos. As organizações realizam grandes investimentos em tecnologias de última geração para proteger seus ambientes e sistemas que manipulam as informações contra acessos não-autorizados, porém de nada adiantará se o fator humano for deixado em segundo plano. É justamente nesse ponto que o Engenheiro Social atua para poder ter acesso as informações confidenciais das organizações.

Para evitar que esse tipo de situação ocorra é necessário criar políticas de segurança e disseminá-las para que seus colaboradores possam ter uma referência sobre o que é segurança da informação, quais informações são confidenciais e de conhecimento público, o que eles

devem fazer e a quem recorrerem em caso de dúvida sobre os riscos presente em determinadas situações, ou seja, é uma diretriz que visa diminuir as chances de que informações estratégicas saiam de dentro das organizações em um simples telefonema.

Como disse Kevin Mitinick, não existe tecnologia que evite um ataque de um Engenheiro Social, portanto é necessário um treinamento contínuo para que as pessoas sempre saibam quais são as novas técnicas utilizadas e como lidar com cada uma delas.

6. Referências Bibliográficas

[1] MARCELO,Antonio;PEREIRA,Marcos. **A Arte de Hackear Pessoas.** Rio de Janeiro: Brasport, 2005.

[2] MITNICK, Kevin D.; SIMON, William L. **Mitnick:** A Arte de Enganar. São Paulo: Pearson Makron Books, 2003.

[3] PEIXOTO, Mário C. P. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006.

[4] REZENDE, Denis A. **Planejamento de Sistemas de Informação e Informática:** guia prático para planejar a tecnologia da informação integrada ao planejamento estratégico das organizações. 3ª Ed. São Paulo: Atlas, 2008.

[5] SÊMOLA, Marcos. **Gestão da Segurança da Informática:** Uma Visão Executiva. 10ªed. Rio de Janeiro: Elsevier, 2003.

[6] MENEZEZ, Heleno, Leonardo, JACOBIMO, Moises e Wladys. **O Fator Humano na Segurança da Informação.** 2004

[7] CAIADO, Marcelo. **Engenharia Social e o Fator Humano na Segurança da Informação.** 2008.

[8] ARAUJO, Eduardo. **A Vulnerabilidade Humana na Segurança da Informação.** 2005

[9] UTFPR. **Apostila Gestão de Segurança da Informação.**