ENGENHARIA SOCIAL: O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO.

Cel R1 Abner de Oliveira e Silva(*)

RESUMO

Este trabalho tem por finalidade abordar o assunto Engenharia Social como um dos fatores que mais comprometem não só a segurança da informação como a própria segurança organizacional. O tema será abordado de uma forma genérica, e não unicamente direcionado para o Exército Brasileiro, por se considerar que a atividade em pauta pode ser desenvolvida para burlar a segurança de qualquer tipo de instituição, da mais humilde à mais complexa. É necessário apenas que haja um produto compensador, seja ele um bem material ou mesmo algo intangível, como uma informação, principalmente se ela tiver um valor estratégico. O trabalho será desenvolvido com base em uma revisão bibliográfica, da qual resultarão evidenciados alguns conceitos básicos, a saber: a importância da informação no mundo moderno, a contextualização da segurança da informação em relação à gerência da informação e uma análise com enfoque comportamental da Engenharia Social. Na conclusão, será mostrado o quão importante é o investimento na conscientização dos integrantes da organização no que diz respeito aos cuidados a serem tomados no manuseio e na disponibilização das informações organizacionais, por mais simples que elas possam ser.

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

ABSTRACT

This paper aims at approaching the Social Engineering issue as one of the factors that compromise both the security of information but also the organizational security itself. This approach will not be exclusively directed to the Brazilian Army but treated in a generic way because we assume the kind of activity herein studied can be developed to cheat the safety of any Institution, no matter how complex it is, provided that there is a worthwhile product, either concrete or intangible, such as a piece of information, especially if the product has an intrinsic strategic value. This work will be developed based on a bibliographic review in which some rudimentary concepts concerning the importance of the information in the contemporary world, the contextualization of the information security in relation to the information management and an analysis focusing on behavioral Social Engineering elements will be highlighted. In conclusion, we will show how important it is to invest in convincing the members of the organization of the procedures to be taken when dealing with or sharing even the least relevant organizational data.

Key words: Information; Information Security; Social Engineering

1 INTRODUÇÃO

Há muito tempo, o mundo precisava da força física do ser humano para se mover. Depois, passou a ser movido a vapor, a querosene, e a

eletricidade. Na atualidade, ele se movimenta impulsionado pelas informações.

Naquele tempo, as distâncias eram enormes. Apesar das distâncias físicas não se alterarem, à medida em que se sucediam as inovações tecnológicas, surgia e crescia a sensação de que os espaços iam sendo encurtados. Se um dia os Templários levaram anos para se deslocarem entre as regiões atualmente conhecidas como França e Israel (Caparelli, 2003), hoje essas distâncias podem ser cobertas em horas pelos modernos meios de transporte e instantaneamente pelas informações transmitidas pela Rede Mundial de Computadores, a Internet.

Ao estudarmos a história da evolução humana, podemos constatar que o ritmo dessa evolução foi sendo modificado conforme aumentava a disponibilização da informação, ou seja, esta última sempre foi um vetor de progresso e desenvolvimento.

Na sociedade globalizada, informatizada e quase totalmente integrada por intermédio da tecnologia de rede, a informação passou a se constituir em um dos principais ativos organizacionais e em fator de diferencial competitivo. Por esse motivo, a informação passou a merecer uma gestão mais específica que, entre outras coisas, contemplasse a garantia da segurança do capital intelectual.

Entretanto, se a mente do homem pode criar coisas maravilhosas, também pode criar ferramentas que ameacem a integridade dos recursos informacionais, sejam eles: equipamentos, programas, sistemas ou mesmo pessoas. Dentre essas ferramentas, enfoca-se, no presente artigo, a interferência humana que, com o emprego da técnica da Engenharia Social, tem se destacado mais recentemente como uma das grandes fontes de obtenção de informações controladas e essenciais.

Assim, o presente artigo foi desenvolvido com o objetivo de evidenciar, mediante uma revisão bibliográfica, a necessidade da adoção de medidas preventivas de proteção e preservação do capital intelectual das organizações, investindo na capacitação e no treinamento dos recursos humanos, visando, principalmente, precaver-se da ação dos invasores virtuais, *hackers* e engenheiros sociais.

Para atingir esse objetivo, foi estabelecida uma estrutura de tópicos que, inicialmente, aborda a informação no contexto da evolução mundial e na sociedade contemporânea, ao que se segue uma exposição sobre o valor patrimonial atribuído à informação no mundo moderno. Em seguida, passa-se a tecer comentários sobre a importância da Gestão da Informação para que esta possa ser utilizada convenientemente como elemento fundamental do processo decisório. Nos tópicos seguintes, serão tratadas as questões da segurança da informação e da Engenharia Social. O trabalho será finalizado com algumas conjecturas sobre o poder da persuasão, capacidade intrínseca ao bom Engenheiro Social.

2 A SOCIEDADE DA INFORMAÇÃO

Já há quase trinta anos, Alvin Toffler, no seu livro “A Terceira Onda”, mostrou o surgimento de uma nova sociedade, sucessora da sociedade industrial, que possuía características comportamentais revolucionárias, decorrentes, em parte, das novas tecnologias surgidas no mundo. Ele também mostrou que as diversas etapas do processo evolutivo da humanidade tinham

"tempos" diferenciados, quando escreveu:

> *A Primeira Onda de mudança – a revolução agrícola – levou milhares de anos para acabar. A Segunda Onda – o acesso à civilização industrial – durou apenas uns poucos 300 anos. Hoje a História é ainda mais acelerativa e é provável que a Terceira Onda atravesse a História e se complete em poucas décadas. (Toffler – 1985. Pág 24)*

Muitos são os autores que adotam a expressão "Sociedade da Informação" para caracterizar o *modus vivendi* do mundo pós-industrial, abstraindo, obviamente, os demais fatores indicados por Toffler e priorizando o aspecto informacional. De qualquer forma, para esses autores, este novo mundo é um mundo acelerado, digitalizado, globalizado, no qual o tempo é cada vez mais escasso para todas as atividades que temos que desenvolver, e teria surgido com o advento do computador.

Historicamente, podemos mapear, sem grandes dificuldades, uma série de acontecimentos que demonstram o conceito temporal apresentado por Toffler, em que, a cada passo, um novo ritmo, ainda mais acelerado, é aplicado ao processo evolutivo. Assim, podemos listar a imprensa de Gutemberg, a máquina a vapor, a eletricidade etc.

Em termos de evolução dos meios de armazenamento e manipulação das informações, os principais eventos estão ligados a nomes como Pascal, Leibniz, Charles Babage, Hollerith. Além disso, dois fatos são inquestionavelmente delimitadores de etapas evolutivas do novo mundo globalizado e informatizado: a criação dos computadores e o nascimento da tecnologia de rede.

Se o primeiro permitiu que as informações fossem digitalizadas e, em consequência, passassem a ser processadas de forma muito mais eficiente, potencializando, de maneira exponencial, o seu valor, o segundo acabou com as distâncias que nos separavam e ampliou, ainda mais, e de forma redundante, aquele potencial, por meio da internacionalização de dados locais e do seu processamento compartilhado.

Como Marcelo Siqueira mostra em seu livro "Gestão Estratégica da Informação": "...a velocidade de movimentação da informação tornou-se absurdamente alta. E estas mudanças estão transformando o mundo corporativo em um ambiente altamente volátil".

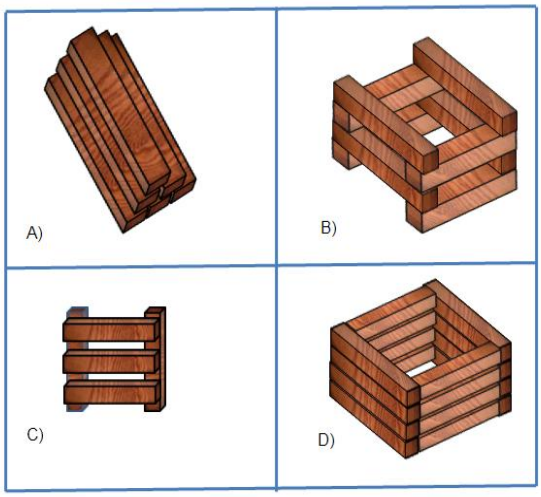
Graças a essas tecnologias, hoje, o mundo está acessível a um "clique". Somos quase deuses, onipresentes. Conseguimos estar em todo o globo, em qualquer e a todo momento. Qualquer notícia chega a nós em frações de segundo. Somos quase deuses, oniscientes. Tudo sabemos! Ou podemos ficar sabendo, uma vez que atualmente a informação nos é disponibilizada de forma ostensiva e intensiva, por intermédio dos meios de comunicação global, principalmente a Internet.

Na verdade, é possível inferir a existência de uma correlação entre o advento de novas tecnologias e as mudanças comportamentais da sociedade, capaz de induzir a uma espiral – quem sabe infindável – de desenvolvimento social e científico, em que um influencia e/ou condiciona o outro.

Sabe-se, ainda que intuitivamente, que a manipulação adequada de informações gera conhecimento. Se a informação pode ser definida como um dado acrescido de contexto, relevância e propósito (Siqueira – 2005), é a congruência de vários fatores, como vivência pessoal e interpretação, que permite a transformação da

informação em conhecimento. E foi em consequência da aplicação do conhecimento que o mundo evoluiu. Vários são os fatos que comprovam a necessidade humana de registrar informação, de transmitir conhecimentos para gerações futuras, tentando garantir que estas informações, estes conhecimentos gerados ao longo dos tempos, não se percam e possam ser reutilizados como base de novas pesquisas e fonte de novos conhecimentos, criando, assim, um círculo vicioso, infinito, do qual resulta o progresso da humanidade.

A figura e a legenda a seguir ilustram os conceitos explicitados acima.



Definir e organizar os relacionamentos entre os dados gera informação, ou seja, definir diver-sos relacionamentos resulta em diferentes informações. Aqui, a madeira pode ser organizada de várias maneiras para criar dois tipos de estruturas – degraus para assento (A) e um caixote (B). Diferentes dados podem ser adicionados para redefinir os relacionamentos e agregar valor.

Adicionando pregos (novos dados), a madeira transforma-se em uma escada (C) ou em uma caixa (D), informações mais valiosas. (adaptada de Stair & Reynolds – 2002 – pag 5)

A preocupação da humanidade com a geração, o armazenamento e a transmissão de informação e de conhecimento parece-nos ser bastante evidenciada ao considerarmos que a necessidade de transportar e conservar informações e conhecimentos fez com que o homem passasse a fazer uso de traços (desenhos e rabiscos) para representar suas ideias, seus pensamentos, em complementação ao uso dos mais antigos e universais processos de comunicação de que se tem notícia: o gesto e a fala.

Na Pré-história, o homem desenhava nas paredes das cavernas, transmitindo seus feitos, suas ideias, seus desejos e necessidades. Mais tarde, passou a representar as “palavras” por intermédio de simbologia gráfica pré-definida, e os 22 símbolos do alfabeto fenício deram origem às 21 consoantes do alfabeto latino, às quais, posteriormente, as vogais foram acrescidas, pelos gregos. (Jhon Man 2002)

Poderíamos tecer ainda muitas outras considerações sobre os processos de coleta, geração, seleção, retenção, transmissão e reutilização de informações e conhecimentos. Embora as caracterizações desses processos pudessem nos ajudar na compreensão da evolução sócio-cultural e político-econômica da humanidade, vamos nos limitar, nesse momento, a concluir que conseguimos demonstrar, com

suficiência, não só a importância da informação e do conhecimento para o nosso processo evolutivo, mas também que a transmissão de conhecimentos adquiridos é uma tarefa intuitivamente tão importante que nos motiva a uma consequente preocupação com a proteção e a preservação dessas informações.

3 O VALOR DA INFORMAÇÃO

Segundo Edison Fontes, a informação sempre foi um bem muito importante para qualquer organização. Há alguns anos, os dados mais importantes da empresa podiam ser guardados "a sete chaves" no interior de algum armário ou gaveta. Modernamente, a quase totalidade das informações, principalmente as de valor estratégico, está digitalizada e armazenada em Estações de Trabalho (computadores pessoais) ou em Servidores (computadores de uso coletivo) acessíveis, todos eles, por intermédio da Rede Mundial de Computadores. (Fontes – 2008)

Alvin Toffler já ressaltava, em 1980, a importância da informação, dizendo que ela "...é tão importante, talvez até mais, do que a terra, o trabalho, o capital e a matéria-prima. Em outras palavras, a informação está se tornando a mercadoria mais importante da economia contemporânea". (Toffler, 1980)

Houve um tempo em que a humanidade lutava pela posse da terra, depois passou a disputar os meios de produção. Hoje o que importa é o acesso à informação.

A informação é diferente de outros produtos de consumo ou bens duráveis. Ela não é destruída ou perde seu valor só por ser utilizada por alguém. Seu valor estratégico pode até ser diminuído se alguém a usa ou com o passar do tempo, mas, em outros casos, ele também pode ser incrementado pelo uso e disseminação. Da mesma forma, a utilização da informação por vários usuários normalmente agrega mais valor a ela ao invés de deteriorá-la.

Marcos Sêmola destaca a importância da informação para o mundo dos negócios quando, no seu livro "Gestão da Segurança da Informação", caracteriza o uso desse ativo empresarial como ferramenta para a obtenção de melhora da produtividade, redução de custos, aumento de competitividade e de apoio ao processo decisório, escrevendo o seguinte:

> *Há muito, as empresas têm sido influenciadas por mudanças e novidades que, a todo momento, surgem no mercado e provocam alterações de contexto. A todo momento surgem descobertas, experimentos, conceitos, métodos e modelos nascidos pela movimentação de questionadores estudiosos, pesquisadores, executivos que não se conformam com a passividade da vida e buscam a inovação e a quebra de paradigmas, revelando – quase que frequentemente, como se estivéssemos em um ciclo – uma nova tendência promissora.*
>
> *Se resgatarmos a história, veremos diversas fases, desde as Revoluções Elétrica e Industrial..., passando pelos momentos relacionados à reengenharia, à terceirização e, mais recentemente, os efeitos da tecnologia da informação aplicada ao negócio. (Sêmola – 2003 – pag 1)*

Neste mundo globalizado e integrado da Sociedade em Rede, como a chama Castells (2003), a atividade empresarial é desenvolvida em uma sequência de momentos de tomada de decisão, em que todas as organizações, sejam elas de que tipo forem, tomam as suas decisões apoiadas em informações, fator decisivo e indispensável, tanto no ambiente interno quanto no relacionamento com o mundo externo à organização.

Peter Drucker, citado por Braga, em seu artigo "A Gestão da Informação", defende a ideia de que a informação é a base de um novo tipo de gestão, no qual o binômio capital/trabalho é substituído pelo novo binômio informação/conhecimento como fator determinante do sucesso empresarial e como chave da produtividade e da competitividade.

Alguns autores defendem a ideia da criação de condições que permitam e promovam a identificação e o compartilhamento dos conhecimentos produzidos e acumulados na organização, sejam de origem individual ou corporativa, explícitos ou tácitos, de tal forma que eles não se percam ou não fiquem disponíveis somente para uma minoria, pois, segundo Drucker (citado por Siqueira – 2005), o conhecimento é o bem capital mais importante das empresas que pretendem sobreviver nesta nova realidade.

Corroborando a posição acima exposta, Siqueira assim se expressa:

> *Encontrar processos eficientes de disponibilização e manipulação de informações e disseminação, armazenamento e criação de conhecimento pode ser um diferencial importante para todos aqueles que procuram por vantagens competitivas sustentáveis no mundo globalizado. (Siqueira – 2005).*

As empresas modernas têm seus processos gerenciais apoiados em uma grande variedade de sistemas de informações, que permitirão que as decisões estratégicas sejam tomadas nas melhores condições possíveis, com base em informações de qualidade, consistentes e confiáveis, disponibilizadas oportunamente.

Como nos mostra Laudon:

> *Nenhum sistema rege sozinho todas as atividades de uma empresa inteira. As empresas têm diferentes tipos de sistemas de informação para enfocar diferentes níveis de problemas e diferentes funções dentro da organização. (Laudon, 1999, pag 26)*

A figura a seguir ilustra a complexidade referida por Laudon no parágrafo anterior.

(Fonte: Laudon, Kenneth C.; Laudon, Jane Price. Sistemas de Informação com Internet. Rio de Janeiro: LTC, 1999).

Se são muitos os sistemas, maior ainda é o número de informações necessárias ao funcionamento deles, do que se pode inferir que o valor da informação é definido em função da maneira como ela ajuda os homens a tomarem suas decisões, ou seja, ela é valorizada, entre outras coisas, em função de: precisão, oportunidade, confiabilidade, relevância e

complexidade.

Em Stair e Reynolds (2002), encontramos uma tabela bastante interessante sobre as características da Informação Valiosa, na qual estão listadas, além das já citadas, as saeguintes: simplicidade, pontualidade, acessibilidade e segurança.

4 A GESTÃO DA INFORMAÇÃO

O mundo cresceu, o mundo mudou, o "Seu Manel", dono do "Armazém da Esquina", que, nos anos 60, controlava suas informações com um lápis atrás da orelha e um caderninho de anotações em que registrava os nomes e saldos de todos os seus clientes – pasmem! ele conhecia a todos!!! –, que controlava seu estoque com um olhar, que possuía fornecedores aos quais se mantinha fiel, viu a população crescer, viu a vila se transformar em bairro, viu as casas virarem prédios, viu surgirem novos fornecedores que agora, em muitos casos, ofereciam vantajosas condições para que ele abandonasse seus fornecedores tradicionais.

O mais importante, dentre todas as mudanças testemunhadas por "Seu Manel", foi ver as pessoas passarem a não ter mais tempo para esperar por um atendimento "personalizado", mas demorado. E para não perder o seu "comércio", o dono do armazém, acompanhando as mudanças, virou dono do mercado "Manoel & Cia.", investiu em tecnologia, comprou um computador, cadastrou os seus fregueses, organizou sua loja em departamentos – limpeza, verdura, bebidas, padaria etc. Suas despesas aumentaram e, com isso, a necessidade de lucro passou a ser uma preocupação maior. Era preciso estar "ligado" às informações de novos produtos, preços e serviços. Era preciso contratar funcionários, pois ele sozinho já não conseguia mais administrar tanta coisa ao mesmo tempo. Era preciso controlar, gerenciar as informações.

A transformação do mundo não se deu após os anos 60 e muito menos foi tão simplória quanto a modernização do "Seu Manel", mas a caricatura acima serve para ilustrar o processo de mudança a que foram submetidas as empresas e o aumento da importância do gerenciamento da informação para o mundo empresarial.

A informação é um ativo que precisa ser gerenciado, e isso envolve investimentos, recursos, pessoas, máquinas e tempo. (Siqueira – 2005). Consequentemente, a Gerência Estratégica da Informação, como nos mostra Costa (2008), abrange as gerências de Tecnologia da Informação (TI), de Pessoas, do Conhecimento e da Segurança da Informação, caracterizando-se como uma atividade multidisciplinar que permeia todos os setores da organização considerada.

Como já vimos, a informação é tratada como o ingrediente básico, do qual dependem os processos decisórios das organizações (Grewood citado por Braga), e, por isso, merece um tratamento gerencial que garanta a sua disponibilização oportuna, de forma quantificada e apropriadamente qualificada, com o emprego de sistemas desenvolvidos em consonância com as necessidades organizacionais, constituindo-se em diferencial competitivo.

O mundo moderno, globalizado, exige que as empresas saibam não só usar as informações obtidas, mas também desenvolver novas maneiras de potencializarem este recurso, de modo que se tornem mais eficientes, mais competitivas.

Esse é o objetivo da Gestão da Informação.

Pode-se verificar que o engenheiro e mestre em administração Heitor Lins Peixoto, assessor da presidência da Usiminas, no prefácio do livro "Gestão da Informação nas Organizações", de Wilson Martins de Assis, afirma que:

> *O desenvolvimento da competência essencial de uma empresa passa, necessariamente, pela qualidade da informação que ela consome – considerando aqui a informação como importante insumo do conhecimento e como um diferencial competitivo –, pois é com base em informações confiáveis e bem elaboradas que os dirigentes organizacionais podem se preparar para desenvolver estratégias capazes de criar valor para seus públicos relevantes. Portanto, um dos principais componentes para a conquista da competitividade em nível global é, sem dúvidas, a construção de um sistema que seja eficaz na busca de informações e na disseminação adequada destas no âmbito da organização. (Assis – 2008).*

O mundo globalizado, ao qual nos referimos anteriormente, tem exigido das empresas uma reação ágil e qualitativamente diferenciada frente aos estímulos oriundos do ambiente externo. Para tanto, as organizações se veem obrigadas a tratar todo o fluxo informacional, desde a busca até o descarte, considerando a informação como um recurso valioso e indispensável, que precisa ser gerido com o máximo de competência e eficiência, priorizando-se a oportunidade, a qualidade e a disponibilidade da informação.

A seleção dos dados que serão transformados em informações cruciais para um processo decisório exitoso só pode ser feita, atualmente, de maneira eficiente, com o uso de tecnologia apropriada. Entretanto, a simples aquisição de equipamentos não atende plenamente às necessidades da empresa. O computador é somente uma ferramenta de trabalho com a qual se pode otimizar os dados coletados. Essa ferramenta deve ser utilizada de forma integrada, como um dos componentes essenciais dos chamados Sistemas de Informações Gerenciais (SIG).

Os Sistemas de Informações Gerenciais possibilitarão ao administrador responder de forma plenamente satisfatória ao mercado atual – dinâmico e globalizado –, desde que tenham sido desenvolvidos três perspectivas básicas: a organização (estrutura, cultura e processos), os recursos tecnológicos disponíveis e as pessoas que, de acordo com Laudon (1999), devem cooperar e ajudar-se mutuamente, ajustando-se e modificando-se ao longo do tempo para otimizar o desempenho do sistema.

Sistema de Informação

Um Sistema de informação deve observar, de forma equilibrada, a tríade:

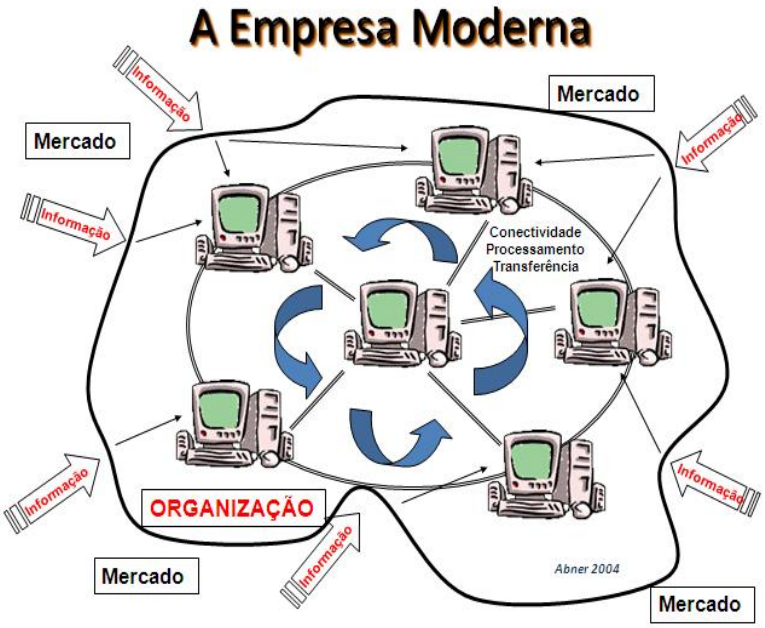
1. **Organização**
2. **Tecnologia**
3. **Pessoas**

(Fonte: Laudon, Kenneth C.; Laudon, Jane Price. *Sistemas de Informação com Internet*. Rio de Janeiro: LTC, 1999).

Além de definir as políticas da empresa, a principal função de um administrador é tomar decisões que proporcionem melhorias nos processos produtivos da organização e que tragam redução das despesas e maximização de lucros.

Ainda no artigo de Braga, constatamos que o referido autor afirma que as Tecnologias da Informação (TI) impulsionam o progresso, conduzem à inovação, aumentam a riqueza e atraem novos investimentos.

De acordo com Batista (2004), é possível obter-se uma visão mais apropriada do universo no qual a organização está inserida, quando a manipulação do conjunto de informações disponíveis no ambiente externo com atuação direta sobre a organização é feita com a ajuda de meios eletrônicos (TI), agindo de forma integrada por intermédio de conectividade, processamento e transferência de dados. Isso também pode ser traduzido como vantagem competitiva.



Então, podemos concordar com Wilson (citado por Braga) quando ele define Gestão da Informação como a gestão eficaz de todos os recursos de informação relevantes para a organização, com uso massivo da Tecnologia da Informação (TI), tenham sido eles gerados em âmbito interno ou externo à empresa. Mais uma vez concordamos com Braga ao dizer que a gestão da informação tem como objetivo maior apoiar a política global da empresa.

É preciso também ter em conta que, qualquer que seja o porte da organização considerada, dificilmente ela terá todas as suas atividades geridas por um único sistema. Para gerenciá-la convenientemente, serão necessários vários subsistemas especialistas que contemplem cada uma das áreas de gerenciamento da empresa e que traduzam os processos específicos nos níveis Estratégico, Tático e Operacional. Sistematizar o uso da informação significa, portanto, criar e garantir um fluxo constante e confiável dessa informação pela estrutura organizacional.

5 A SEGURANÇA DA INFORMAÇÃO

Ao atingirmos esse ponto da matéria, imaginamos ter conseguido deixar bem claro alguns pontos básicos de raciocínio, essenciais para a continuação do trabalho. São eles:

a) as organizações possuem informações que permitem gerar conhecimentos e, junto com estes, constituem-se em diferencial competitivo;

b) as organizações modernas dependem de recursos tecnológicos para concretizarem seus negócios;

c) as organizações possuem Sistemas de Gerenciamento e de Apoio à Tomada de Decisões essencialmente baseados em informações estratégicas;

d) as informações e os conhecimentos gerados são patrimônios relevantes da empresa; e

e) as organizações modernas são organismos vivos inseridos na rede mundial de computadores, e, nesse ambiente, são participantes ativos.

Revista INFO de julho de 2009

"A TECNOLOGIA DO MUNDO DO CRIME"
Google Earth, VoIP e câmeras de vídeo entram para o arsenal das quadrilhas.

Edison Fontes (2006), na abertura do primeiro capítulo do seu livro "Segurança da Informação – O usuário faz a diferença", apresenta a seguinte citação: "A informação, independentemente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos."

Segundo o dicionário Aurélio, proteger é "preservar do mal", ou seja, proporcionar meios que garantam a integridade e a perenidade do bem protegido.

Dessa forma, questão que agora se apresenta é: Como proteger a informação e/ou o conhecimento gerado, a partir dela, na organização?

No passado, antes do advento da tecnologia de rede, quando a informação era armazenada em papel ou em computadores que funcionavam isoladamente ou, no máximo, nos *mainframes* acessados pelos chamados "terminais burros", o

uso de crachás, a manutenção de portas fechadas e, por vezes, a instalação de câmeras de vídeo, ao controlarem o acesso às instalações sensíveis, eram bastantes para prover a segurança necessária. Apesar disso, não foram poucos os casos de roubo ou de uso indevido de informações privilegiadas.


Fonte: Google/imagens

Hoje, entretanto, as tecnologias disponíveis permitem que os criminosos penetrem nas organizações de forma virtual, a distância, por acesso remoto, via Internet.

Além disso, há que se considerar que a segurança da informação não deve ficar restrita ao aspecto do furto. Se a informação é um bem, um patrimônio relevante para a organização, ela deve ser preservada, também, das possibilidades de perda, dano ou alteração, decorrentes tanto de causas naturais como de ação humana, seja ela intencional ou não.

Então, podemos deduzir que as informações e os conhecimentos organizacionais, assim como seus repositórios, estão sujeitos a uma série de ameaças que podem ser, como descrito por Sêmola (2003), classificadas quanto a sua intencionalidade e divididas em grupos da seguinte maneira:

• **Naturais** – aquelas decorrentes de fenômenos da natureza, como enchentes, terremotos, tempestades etc.

• **Involuntárias** – as inconscientes, que podem ser causadas por desconhecimento, acidentes, erros etc.

• **Voluntárias** – as decorrentes de ação de agentes humanos, como invasores, espiões, ladrões, incendiários etc.

A segurança absoluta ou perfeita é uma utopia. Convém, portanto, que se evidencie que as ameaças só se concretizam, ou seja, só produzem efeitos nocivos, quando exploram ou encontram condições favoráveis – vulnerabilidades.

Logo, as vulnerabilidades permitem a ocorrência de incidentes que podem afetar negativamente o negócio da empresa, causando, danos, prejuízos ou repercussões, no mínimo indesejáveis, para os produtos, para a imagem da empresa ou mesmo para os clientes.

Essas vulnerabilidades podem ser físicas (instalações), técnicas (equipamentos e aplicativos), processuais (normas, definições e configurações) ou humanas (comportamentais). Para a manutenção da segurança, é imprescindível que se consiga identificá-las corretamente, a fim de que possam ser estabelecidas as medidas necessárias à anulação ou à minimização dos seus efeitos.

Essas medidas tanto poderão ser de caráter preventivo como corretivo. Enquanto as primeiras têm o objetivo de evitar que algum mal ocorra, as corretivas, normalmente, só serão adotadas após o evento ter ocorrido e o dano já ter sido causado. Porém, ainda assim, não devem ser desprezadas, pois sua adoção evitará que o problema se repita.

Aprender com os erros também demonstra sabedoria.

Marcos Sêmola (2003) refere-se à deficiência de percepção do problema da segurança da informação por vários executivos e

organizações como a "*Visão do Iceberg*", quando compara a pequena fração do bloco de gelo exposto acima da linha de superfície do mar ao enfoque puramente tecnológico dado por aqueles ao assunto. Nos dias de hoje, a informação não fica mais restrita a áreas específicas ou a determinados processos, ela agora flui com dinamismo por toda a estrutura organizacional de forma compartilhada, sendo alvo de interferências físicas e humanas.

Por esses motivos, é imperativo, para que possam ser alcançados resultados eficazes, tratar um Sistema de Gerenciamento de Segurança da Informação de forma integrada e multidisciplinar, devendo, portanto, balancear, de forma adequada, segurança física, técnica, processual e pessoal, ou seja, é preciso encarar a Segurança da Informação como um processo de gerenciamento e não como um processo puramente tecnológico.

Como nosso objetivo principal é evidenciar a participação e a interferência humanas nos processos que visam à segurança das informações organizacionais, vamos, mais uma vez, buscar o apoio de Marcelo Siqueira (2005) e trazer quatro assertivas por ele expostas:

"...a administração da informação tem como principal aliada a análise originada no conhecimento humano..." (Siqueira 2005, pag 29);

"O trabalho do gestor de informação não é baseado em ciências exatas, mas em relacionamentos humanos e sistemáticos" (Siqueira 2005, pag 30);

"Negligenciar o potencial humano é o mesmo que negligenciar a própria organização, pois esta nada mais é do que o suporte humano, que garante o funcionamento de seus processos e o cumprimento de missões, objetivos e visões" (Siqueira 2005, pag 41); e "... o foco de qualquer problema não deve ser a tecnologia, e sim a melhor utilização das habilidades individuais nos processos do negócio..." (Siqueira 2005, pag 43).

A adoção de rígidas medidas de segurança tecnológica não surte o efeito desejado se os funcionários deixam portas abertas, computadores com acesso liberado, pastas largadas sobre as mesas ou trocam "confidências" sobre decisões estratégicas de forma promíscua.

Vários são os autores que consideram a conscientização e o comprometimento dos funcionários como uma das melhores ferramentas de segurança da informação, principalmente quando constatamos que são eles que fazem com que a organização funcione.

De acordo com a maioria dos autores que tratam do assunto, a segurança da informação tem por objetivo garantir três aspectos ou princípios, julgados básicos, a saber:

•DISPONIBILIDADE – garantia de acesso aos usuários, quando necessário;

•CONFIDENCIALIDADE – grau de sigilo atribuído ao conteúdo da informação e utilizado para especificar quem pode acessá-la; e

•INTEGRIDADE – manutenção da exatidão da forma e do conteúdo originais da informação.

Os dois primeiros aspectos têm características defensivas e estão relacionados com a proteção do negócio, enquanto a integridade é fator imprescindível para o processo de tomada de decisão.

Como a Segurança da Informação deve ser responsabilidade de todos dentro da organização, desde o mais alto nível ao colaborador mais recentemente contratado, passando por todos os patamares hierárquicos intermediários, é

importante que haja investimento na capacitação e conscientização dos funcionários no que tange às operações de todo o ciclo de vida da informação, ou seja, manuseio, armazenamento, transporte e descarte de informações.

Por mais que se adote e implemente recursos tecnológicos para a proteção das informações, não se pode desprezar a capacidade inventiva, a criatividade humana. A cada nova tecnologia de segurança inventada, logo aparece alguma outra para burlá-la.

Edison Fontes (2006) define Segurança da Informação como "o conjunto de orientações, normas, procedimentos e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada". Ele ainda alerta que para a eficácia da proteção da informação, os conceitos e regulamentos relativos ao assunto devem ser compreendidos e seguidos por todos os usuários. (Fontes 2006, Pag.11)

Segundo pesquisa divulgada pela Módulo *Security Solutions*, em 2001, e citada por Siqueira (2005), são duas as principais ameaças às informações nas empresas: vírus e funcionários insatisfeitos.

No artigo "Segurança: questão de sobrevivência do negócio", André Correia[1] nos mostra que, de acordo com pesquisa realizada pelo CSI[2], 71% dos incidentes de segurança são causados pelo pessoal interno.

Todos os leitores possivelmente já ouviram ou leram a afirmativa de que uma corrente é tão forte quanto o seu elo mais fraco, em especial quando algum autor quer se referir à participação humana no processo de segurança.

E por que o fator humano é considerado o elo mais fraco da segurança?

Em muitos casos, a segurança é apenas ilusória, principalmente quando entram em jogo a credulidade, a inocência ou a ignorância do usuário. Atribui-se a Albert Einstein a seguinte citação: "Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro".

Seria interessante tratar a participação humana como um fator externo à corrente que manipula os seus elos, correta ou incorretamente, decorrendo desta manipulação a longevidade ou a corrosão total deles. Os elos da corrente de segurança são: senhas, *logins*, *firewalls*, criptografia, normas, políticas, regulamentos, antivirus, anti-*spaywares*, *pendrives*, disquetes, CD/DVD, crachás e mais toda a sorte de equipamentos, mídias, documentos, *softwares* e procedimentos que tenham por finalidade prover a segurança deste importante ativo empresarial que é a informação.

---

[1] *Gerente de Planejamento e Consultoria da Open Communications Security. É graduado pela PUC-RJ em Tecnologia em Processamento de Dados e tem especialização em Redes de Computadores.*

[2] *Computer Security Institute*

Abner Junior - 2009

Não se pode negar que, quando as pessoas agem como foi indicado acima, de forma ingênua, estúpida ou indiferente às boas práticas recomendadas pelas normas de segurança, a engenharia social encontra seu meio mais fértil de atuação.

O grande problema para a implementação de procedimentos de segurança é a mudança cultural incômoda que ela promove, uma vez que impõe restrições às "comodidades", às quais os usuários já estavam acostumados e, logicamente, não querem perder. Em consequência, essa implementação deve ser feita de forma gradativa, mas de maneira contínua e permanente, pois resultados significativos só aparecem, efetivamente, em médio e/ou longo prazo.

Sem dúvida, o grau de "desconforto" do usuário será diretamente proporcional ao grau de segurança que se deseja, ou seja, quanto maior o grau de segurança desejado, maior será o controle a ser exercido, maior será a quantidade de restrições, maior poderá ser o desconforto do usuário, maior também será a reação dos usuários à adoção das medidas implementadas. Apesar disso, é preciso entender e não esquecer que segurança não é um problema. Problema é a falta de segurança e o prejuízo que ela pode trazer para a organização.

Então, qual será o grau de segurança a ser adotado? Esta decisão é complexa e deverá ser tomada com muita parcimônia, pois uma política de segurança muito austera poderá causar entraves nos processos produtivos, ao passo que se for muito permissiva poderá expor, desnecessária e indesejavelmente, a organização.

Luís Mirtilo[3], citado por Estela Silva em seu artigo "Especial Sobre Segurança", aponta a engenharia social como um dos grandes vilões da segurança da informação, embora aponte, também, como importantes ferramentas de ataques: os vírus recebidos por *e-mail*, a insatisfação de funcionários, os erros operacionais, a invasão por *hackers*, os acidentes e desastres e, por fim, a espionagem, remota ou local, fatos e procedimentos, que têm a participação ativa, voluntária ou não, dos usuários.

---

[3] *Diretor de operações da Plaut Consultoria*

Acreditamos que seja fácil imaginar as nefastas consequências que adviriam para uma força de defesa –Exército, Marinha, Aeronáutica, Guarda Nacional, Gendarmaria etc. – no caso de uma invasão que destruísse ou alterasse significativamente a base de dados de uma unidade operacional durante uma operação real.

Na atualidade, o exército norte-americano realiza treinamento de seus oficiais no sentido de os capacitar para fazer frente a ataques cibernéticos. Recentemente, foi disponibilizado na página eletrônica do *youtube*, conforme mostrado na imagem acima, um filmete que demonstra esse treinamento.

Fonte:

http://www.youtube.com/watch?v=hDpqruR3vvk

Alguns dados estatísticos mais atualizados sobre ataques virtuais – Guerra Digital – podem ser encontrados no sítio *Zone-H, unrestricted information*, cujo endereço de acesso pode ser (http://www.zone-h.com.br/content/blogcategory/9/11/) ou (http://www.zone-h.com.br/content/view/579/11/).

A Política de Segurança é uma atribuição da organização que a pretende implantar, mas não podemos nos furtar de mencionar dois documentos de referência quanto a esse assunto: as normas ISO[4] 17799 (ISO/IEC 27002) e o COBIT[5].

A ISO/IEC 17799, renumerada em julho de 2007 para ISO/IEC 27002, é uma norma de Segurança da Informação – revisada em 2005 pelas referidas organizações ISO e IEC – composta por um conjunto de recomendações para práticas na gestão de Segurança da Informação, ideal para aqueles que querem criar, implementar e manter um sistema de segurança.

O COBIT é um guia de boas práticas, criado e mantido pelo ISACA[6], que possui uma série de recursos que podem servir como modelo de referência para gestão da Tecnologia da Informação (TI).

A esses documentos, Ferreira e Araujo (2006) assim se referem:

> *Atualmente existem algumas metodologias e melhores práticas em segurança da informação e governança para o ambiente de tecnologia, que são reconhecidas mundialmente e largamente utilizadas como, por exemplo, a NBR ISO/IEC 17799:2005 e o CobiT. (Ferreira e Araujo, 2006, pag 27)*

É verdade que segurança absoluta não existe, mas é necessário que nos preocupemos com a adoção de medidas que dificultem a ação de *hacker* ou de curiosos e garantam minimamente a privacidade dos dados que julgamos confidenciais, sejam eles pessoais ou funcionais, principalmente no ambiente organizacional.

Fontes (2008, pag. 6) apresenta considerações sobre proteção da informação para o executivo da organização. Proteger a informação:

[4] *International Organization for Standardization – Organização Internacional para Padronização*
[5] *Control Objectives for Information and Related Technology*
[6] *Information Systems Audit and Control Association*

a) não é um assunto puramente tecnológico;

b) é uma decisão empresarial;

c) não acontece por milagre;

d) deve fazer parte dos requisitos do negócio;

e) exige postura profissional das pessoas;

f) é liberar a informação apenas para quem precisa;

g) é implementar o conceito de Gestor da Informação;

h) deve contemplar todos os colaboradores;

i) considerar as pessoas um elemento vital; e

j) exige alinhamento com o negócio.

6 A ENGENHARIA SOCIAL

"Botafogo, Rio de Janeiro. Uma aposentada de 79 anos passa sete horas sob tortura psicológica, pendurada ao celular. Criminosos que diziam ter seqüestrado sua sobrinha-neta a induzem a fazer saque em caixas eletrônicos. ***Sabem o nome e hábitos da vítima*** *(grifo nosso). O drama só termina quando a aposentada recebe um contato da mãe da suposta seqüestrada, o que evita que ela entregue o dinheiro aos golpistas.*

Santa Cruz do Rio Pardo, interior de São Paulo. Uma quadrilha clona cartões bancários de cerca de 100 pessoas.." (Revista Info – Julho de 2009 – pag. 62)

Fonte: Google/imagem

O Caderno Digital, distribuído pelo jornal O Globo na segunda-feira, dia 20 de julho de 2009, publicou, na sua página 12, um artigo intitulado "Cibercriminosos de olho na nuvem", que abordava a questão da exploração, por parte desses criminosos, da ignorância e da ingenuidade das pessoas que se utilizam de forma equivocada ou imprudente dos meios tecnológicos disponíveis e ressaltava a participação de ex-funcionários que vendem informações sensíveis à concorrência, como ocorreu, em caso recente, no mundo da Fórmula 1, entre a Ferrari e a McLaren.

Ao pesquisar na literatura pertinente ou "navegar" em artigos disponibilizados na Internet, podemos encontrar várias definições de Engenharia Social. Vejamos algumas delas:

- termo utilizado para a obtenção de informações importantes de uma empresa, por intermédio de seus usuários e colaboradores;
- arte de fazer com que outras pessoas concordem com você e atendam aos seus pedidos ou desejos, mesmo que você não tenha autoridade para tal;
- aquisição de informações preciosas ou privilégios de acesso por "alguém de fora", baseado em uma relação de confiança estabelecida, inapropriadamente, com "alguém de dentro";
- técnicas utilizadas para tirar proveito de falhas que as pessoas cometem ou que sejam levadas a cometer com relação às informações da área de tecnologia da informação;
- técnica de influenciar as pessoas pelo poder da persuasão com o objetivo de conseguir que elas façam alguma coisa ou forneçam determinada informação a pedido de alguém não autorizado;
- método de ataque virtual no qual é aproveitada a confiança ou a ingenuidade do

usuário para obter informações que permitem invadir um micro;

- habilidade de um *hacker* manipular a tendência humana natural de confiança com o objetivo de obter informações por meio de um acesso válido em um sistema não autorizado;
- arte e ciência de persuadir as pessoas a atenderem aos seus desejos; e
- "garimpagem da informações".

Qual a melhor? Qual a mais correta?

A escolha ficará a cargo de cada leitor, mas o que não se pode negar é o fato de a Engenharia Social ser uma atividade conceitualmente ligada à atividade de busca de informação, seja a busca desenvolvida por intermédio de equipamentos eletroeletrônicos (telefone, computador) ou pessoalmente (entrevista ou questionamento).

Outro aspecto que nos parece ter ficado também bastante evidenciado na leitura dos conceitos expostos é a intenção de obter acesso a locais ou produtos normalmente negados ao engenheiro social.

Podemos ainda identificar, no conjunto de definições apresentadas, a utilização e/ou exploração da ingenuidade, da confiança e/ou da boa-fé das pessoas.

É importante destacar que o sucesso no ataque de engenharia social ocorre, geralmente, quando os alvos são pessoas ingênuas ou aquelas que simplesmente desconhecem as melhores práticas de segurança. (Ferreira & Araujo, 2006, pag 92)

Soeli Claudete Klein, no seu trabalho intitulado "Engenharia Social na Área da Tecnologia da Informação", assim se refere à Engenharia Social:

> *A engenharia social atua sobre a inclinação natural das pessoas de confiar umas nas outras e de querer ajudar. Nem sempre, a intenção precisa ser de ajuda ou de confiança. Pelo contrário, pode ser por senso de curiosidade, desafio, vingança, insatisfação, diversão, descuido, destruição, entre outros.*
>
> *A engenharia social também deve agir sobre as pessoas que não utilizam diretamente os recursos computacionais de uma corporação. São indivíduos que têm acesso físico a alguns departamentos da empresa por prestarem serviços temporários, porque fazem suporte e manutenção ou, simplesmente, por serem visitantes. Há ainda um grupo de pessoas ao qual é necessário dispensar uma atenção especial, porque não entra em contato físico com a empresa, mas por meio de telefone, fax ou correio eletrônico. (Klein – 2004, pag 9)*

Já Evaldo Tatsch Junior (2009) mostra-se surpreso em constatar que a engenharia social ainda é um dos meios de maior sucesso para acesso a informações. Ele ressalta que muitas pessoas de elevado nível sóciocultural ainda se deixam enganar por esses vilões cibernéticos, a quem chama de "salafrários virtuais".

A Engenharia Social tem sido tema e preocupação constantes de publicações especializadas, que procuram chamar à atenção os usuários "comuns" dos novos recursos tecnológicos, para que procurem ter mais cautela ao disponibilizarem dados pessoais, funcionais e/ou comerciais.

A revista Info-exame, especializada em assuntos relativos à tecnologia, publicou, na sua edição de julho de 2009, o artigo "A Tecnologia do Crime", no qual se pode ler que "Em muitos casos, funcionários de estabelecimentos comerciais são aliciados e permitem que criminosos instalem dentro do terminal de pagamento um chupa-cabra". De acordo com o mesmo artigo, "chupa-cabra" são dispositivos que memorizam as informações da tarja magnética do

cartão para cloná-los posteriormente. (Revista Info – Jul 2009 – pag. 66)

Outro grande foco de obtenção de informações pessoais, ou mesmo funcionais, são as chamadas redes de relacionamento, às quais o Caderno Digital, do jornal O GLOBO, refere-se da seguinte forma:

> *As redes sociais têm um aspecto sombrio no que tange à segurança da informação. Como a própria web e os dados de identidade dos internautas passaram a ser o alvo dos criminosos digitais nos últimos tempos, Orkut e congêneres não poderiam ficar de fora de sua mira. (Caderno Digital – O Globo – 6 de julho de 2009).*

Ainda tendo como referência o caderno Digital do O Globo, destacamos o artigo, publicado no dia 29 de junho de 2009, denominado "Cuidado com a e-perseguição", em que são apresentados casos de "perseguição digital", do qual extraímos os seguintes trechos:

> *Há alguns anos ela teve a sua vida devassada por um ex-namorado inconformado com o fim do relacionamento. C. começou a desconfiar quando o "ex" mostrou saber quais eram seus compromissos, os lugares aonde planejava ir e até quanto possuía na conta bancária. Assustada, resolveu procurar um consultor de segurança.*
> *- Ela me perguntou: "é possível alguém saber pela internet o que estou fazendo?" – lembra o consultor.*
> *- Eu, por minha vez, perguntei se ele tinha acesso ao computador dela. E descobri que ele tinha dado o PC de presente a ela!*
> *É claro que foi um presente de grego. A máquina tinha vindo preparada com um programa de acesso remoto e um keylogger (dispositivo que grava a digitação).*
> *Resumo da história: através do keylogger e de outras "armas" instaladas no PC, o "ex" de C. pôde reconstituir todos os seus movimentos e capturar seus logins e senhas, inclusive os do banco na internet. Assim, sabia de toda a sua vida.*
> *Na internet, os protocolos de comunicação não são protegidos e a conversa não trafega criptografada, então alguém pode capturá-la e se inteirar de histórias confidenciais.*

A imagem ao lado ilustra mais uma vez a obtenção, por meios ilícitos, de dados confidencias disponibilizados de maneira ingênua e inconsequente, que poderão ser utilizados pelos chamados "cibercriminosos" para coação ou mesmo chantagem.

A imagem, acessada em 25/07/09, está disponível no artigo "Desculpe, Luciana, não funcionou, mande de novo", acessível na URL a seguir: http://www.contraditorium.com/2008/01/28/desculpe-luciana-nao-funcionou-mande-de-novo/.

A imagem também pode ser encontrada na 8ª página de imagens do Google **sob o enfoque da engenharia social,** ou seja:

1) digite "google.com.br";

2) escolha o menu "imagens";

3) digite "engenharia social" na caixa de pesquisa e clique em "ok";

4) escolha a página 8;

5) "voila" – é a primeira imagem que aparece; e

6) clique sobre a imagem e veja o artigo.

No livro de Peixoto (2006), encontramos o Engenheiro Social definido como uma pessoa gentil, agradável, educada, simpática, carismática, criativa, flexível, dinâmica, persuasiva e dona de uma conversa muito envolvente. Como se proteger de alguém assim?

Suas principais ferramentas de trabalho são: telefone, internet, intranet, *e-mail*, *chats*, fax, cartas/correspondência, "spyware", observação pessoal, procura no lixo e intervenção pessoal direta.

Normalmente, possuidor de inteligência privilegiada, o Engenheiro Social vai "somando" todas as informações que, pacientemente, consegue obter nas inúmeras incursões (eletrônicas ou pessoais) aos arquivos da vítima, até conseguir compor um mosaico de informações significativas que o permita construir o perfil social e funcional do alvo e, assim, ter condições de realizar as fraudes que deseja.

Peixoto (2006) ainda apresenta uma interessante definição de Engenharia Social, segundo ele obtida no sítio da Konsultex Informática: "ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar o seu desejo".

A enciclopédia eletrônica – Wikipédia – define Engenharia Social como sendo "o conjunto de práticas utilizadas para obter acesso a informações importantes ou sigilosas, em organizações ou sistemas, por meio da enganação ou exploração da confiança das pessoas", ou, ainda, como "uma forma de entrar em organizações, que não necessita da força bruta ou de erros em máquinas" e que possui a destacada propriedade de "Explorar as falhas de segurança das próprias pessoas que, quando não treinadas para esses ataques, podem ser facilmente manipuladas".

A mesma enciclopédia esclarece que o Engenheiro Social pode se fazer passar por outra pessoa, fingindo ser um profissional que na realidade não é, para explorar as falhas de segurança. Ainda relaciona traços comportamentais e psicológicos que tornam o homem suscetível a ataques de engenharia social. Entre eles, pode-se destacar:

- vaidade pessoal e/ou profissional;
- autoconfiança;

a) vontade de ser útil; e

a) busca por novas amizades.

Falar de Engenharia Social sem falar em Kevin Mitnick é o mesmo que falar de futebol sem falar em Pelé.

Kevin Mitnick é o mais famoso *hacker* do mundo. Ele foi caçado e preso pelo "Federal Bureau of Investigation" (FBI) em 1993 e, depois de passar cinco anos na prisão, ainda cumpriu mais três de liberdade condicional. Atualmente Mitnick é dono de uma consultoria, conferencista e escritor de livros, tendo publicado "A Arte de Enganar" e "A Arte de Invadir". No primeiro deles, Mitnick procura transmitir ensinamentos que sirvam de base para que usuários se previnam contra os possíveis e eventuais ataques desse gênero, contando suas aventuras e peripécias, enquanto no segundo, os ensinamentos são passados com base em experiências vividas por outros *hackers*.

De acordo com Mitnick (2003), ao serem combinadas a inclinação para enganar as pessoas com os talentos da influência e persuasão, chega-se ao perfil de um engenheiro social do qual nem um computador desligado está livre da ação, pois ele é capaz de convencer um colaborador a entrar no escritório e ligá-lo. O referido escritor também destaca que, enquanto os colaboradores de uma empresa não estiverem devida e suficientemente "educados", treinados para não fornecerem informações a estranhos, mais ou menos como nossos pais nos ensinavam nos idos anos 50 e 60, as organizações continuarão sendo alvo do ataque

de vândalos e criminosos tecnológicos.

Ainda segundo Mitnick, alguns desses ataques são sofisticadíssimos, verdadeiras obras de arte em termos de concepção e planejamento, exigindo profundos conhecimentos tecnológicos. Mas, em outros casos, tudo o que o engenheiro precisa fazer é simplesmente pedir a informação desejada.

O atacante pode ainda atuar oferecendo ou pedindo ajuda, vasculhando o lixo ou enviando e-mails. No entanto, ele basicamente aplica, intuitiva ou conscientemente, conhecimentos que lhe permitam explorar sentimentos e/ou emoções, tais como: medo, culpa, descontentamento, vingança, simpatia etc.

Senhas podem ser facilmente "quebradas" (descobertas) com a utilização de programas que são capazes de testar, por exemplo, todas as palavras contidas em um bom dicionário e mais todas as combinações possíveis dos dados de nascimento da vítima e de seus familiares. São muitas as pessoas que, preocupadas em não se esquecerem de suas senhas, usam essas datas para protegerem seus acessos aos mais diversos meios de armazenamento de dados ou se utilizam de uma única senha para todos os acessos.

Qualquer candidato a *hacker* que tenha um mínimo de conhecimento da lógica utilizada pelos informáticos começará a tentativa de quebra de senhas por combinações como "123456..", "abcdef..", "111111...", "00000...".

Os livros de Mitnick nos apresentam uma série de casos explorados muito convenientemente, para mostrar o quão vulneráveis podemos ser, ou estar, a este tipo de ação criminosa, assim como uma série de procedimentos a serem adotados como medida preventiva. Trata-se de leitura obrigatória para todos aqueles que querem aprender alguma coisa sobre exposição e proteção relativas à Engenharia Social.

Ambos os livros, "A Arte de Enganar" e "A Arte de Invadir", estão disponíveis na forma de livros eletrônicos gratuitos e podem ser obtidos com a ajuda de pesquisa direta no Google.

Os Engenheiros Sociais, apesar de serem normalmente classificados como criminosos eletrônicos, podem, entretanto, ser simples captadores de informações, sem nenhum conhecimento de informática. O crime por eles cometido é repassar as informações colhidas àqueles criminosos.

Esses *hackers* são categorizados em tipos que os classificam de acordo com a malignidade de seus atos e suas competências técnicas. Desses tipos cabe destacar:

- Os *Hackers* ou "White hat" – aqueles que após detectarem uma falha na segurança e invadirem uma organização deixam um alerta para que a incorreção seja eliminada. Praticamente fazem a invasão pela satisfação de vencer o desafio de superar as barreiras existentes.

- Os *Crackers* ou "Black hat" – aqueles que possuem praticamente o mesmo nível de conhecimento do tipo anterior, mas diferem dele pelos objetivos realmente criminosos, causando qualquer espécie de prejuízo ao invadido e, se possível, obtendo lucro pessoal.

- Os *Phreakers* – aqueles que, essencialmente, manipulam equipamentos e sistemas de telecomunicações para conseguirem as informações desejadas.

Nem mesmo as Forças Armadas estão livres da ação desses ataques. Afinal, se para alguns

hackers o importante é vencer desafios, como seriam conceituados aqueles que conseguem em uma ação de, aparentemente, extrema ousadia, vencer as barreiras de segurança das organizações que, pelo menos teoricamente, são as mais fortes em termos de segurança? Invadir o pentágono, por exemplo, e simplesmente "plantar" um alerta de invasão traria ao invasor um reconhecimento internacional da sua capacitação tecnológica.

Se por um lado, a internet pode se configurar em grande ameaça corporativa, por outro, ela disponibiliza uma série de arquivos e fontes de consultas com toda sorte de informações sobre a atuação dos "cibercriminosos", possibilitando a todos aprenderem sobre o assunto e se prepararem para fazer frente a esse tipo de ação. São inúmeros os arquivos armazenados nos principais provedores de acesso à internet como, por exemplo, Google, Yahoo e Terra, assim como de filmetes do sítio "youtube", com verdadeiras aulas sobre invasão, engenharia social, "worms", "trojans", vírus, cavalos de troia, captura de senhas, "spyware" e outras dessas tecnologias. Basta acessá-los, aprender e se proteger.

Diante desse cenário, julgamos que o mais importante aspecto relativo à segurança das informações corporativas que merece ser destacado é, inquestionavelmente, a necessidade de capacitação (cognitiva e comportamental) dos usuários dos diversos sistemas da organização, dos gestores e dos manipuladores do capital intelectual da instituição.

Em todo o caso, é preciso estar consciente de que o Engenheiro Social atua baseado em três aspectos, a saber: motivação pessoal (desafio, ganância ou sentimento de aventura), falta de controle da organização (vulnerabilidades) e oportunidade (exploração das vulnerabilidades existentes). Dos três aspectos, o único que não podemos controlar é o primeiro deles, a motivação, por ser estritamente pessoal. Nos demais, temos obrigação de atuar, dificultando ao máximo a ação dos invasores.

Para isso, precisamos pensar em estabelecer alguns níveis de barreiras:

- barreiras físicas (portas, cadeados, trancas);

- controle de acesso (estabelecimento de senhas, perfis de usuário e registro de acesso realizado);

- classificação das informações (grau de sigilo);

- uso de processos de codificação e autenticação (criptografia, certificação digital) das informações que circulam na rede da organização;

- armazenamento distribuído das informações organizacionais; e

- realização periódica de cópias de segurança (*backup*).

De qualquer forma, julgamos também imprescindível não esquecer que o engenheiro social normalmente adota como principal ferramenta de ataque a persuasão, que será o foco do nosso próximo tópico.

Encerramos este tópico com o mais antigo relato que se pode ter da hoje chamada Engenharia Social:

> Ora, Isaac envelheceu, e a vista escureceu-se-lhe, e não podia ver.
> (...)
> Vestiu Jacó com os melhores vestidos de Esaú (...) e com as peles dos cabritos, envolveu-lhe as mãos e cobriu a parte nua do pescoço.
> (...)
> Jacó, tendo levado tudo a Isaac, disse-lhe:
> - Meu Pai!

Ele respondeu: Ouço.

- Quem és tu, meu filho?

Jacó disse:

- Eu sou teu filho primogênito, Esaú.

(...)

Isaac disse:

- Chegue aqui, meu filho, para que eu o apalpe e reconheça se és o meu filho Esaú ou não.

Jacó aproximou-se do pai, e, tendo-o apalpado, Isaac disse:

- A voz verdadeiramente é a voz de Jacó, mas as mãos são as de Esaú.

Issac não o reconheceu porque as mãos peludas eram semelhantes às do mais velho. Portanto, abençoando-o disse:

- Tu és o meu filho Esaú?

Jacó respondeu:

- Eu o sou.

E Isaac o abençoou (...) (A Bíblia Sagrada – Gênesis 27)

7 O PODER DA PERSUASÃO

Fonte: Google/imagem

Com tão pouco tempo precioso para processar tanta informação, nosso sistema cognitivo especializa-se em atalhos mentais. Com extraordinária facilidade, formamos impressões, fazemos julgamentos e inventamos explicações. (...) A finalidade biológica principal do pensamento é nos manter vivos, e não garantir a certeza de nossos julgamentos. Em algumas situações, porém, a pressa nos conduz ao erro. (Myers – 2000, pág. 58)

Todos conhecemos ou já ouvimos relatos sobre pessoas que se destacam por conseguirem, surpreendentemente, tudo o que desejam. São aquelas pessoas para as quais tudo parece sempre "dar certo". E o mais estranho é que, em muitos casos, elas nem parecem ser tão competentes, inteligentes ou trabalhadoras, mas estão sempre alcançando seus propósitos.

Se observarmos um pouco mais atentamente a conduta de vida dessas pessoas, talvez possamos identificar nelas uma incrível capacidade, muitas vezes natural, inata, de falar aquilo que deve ser dito, da maneira mais agradável, no momento oportuno e para a pessoa certa. Essa capacidade conquista pessoas, constrói relacionamentos e permite que o comunicador influencie o ouvinte, que passa a respeitá-lo, admirá-lo e até apoiá-lo na consecução dos seus objetivos.

Essa capacidade é denominada persuasão e, como já dissemos anteriormente, constitui-se na principal ferramenta de ataque dos engenheiros sociais na maioria das situações. É através dela que eles nos induzem a um erro de julgamento que nos faz vê-los como pessoas confiáveis, o que obviamente não o são.

Consultando a enciclopédia eletrônica Wikipédia, verificamos que a Persuasão é definida como "uma estratégia de comunicação que consiste em utilizar recursos lógico-racionais ou simbólicos para induzir alguém a aceitar uma ideia, uma atitude, ou realizar uma ação", ou ainda, "o emprego de argumentos, legítimos ou não, com o propósito de conseguir que outro(s) indivíduo(s) adote(m) certa(s) linha(s) de conduta, teoria(s) ou crença(s)".

Então podemos entender que o engenheiro social fará uso de todo seu poder de argumentação, consciente ou intuitivamente, para nos convencer a lhe franquear o acesso às informações que ele deseja.

Se houver competência técnica por parte do invasor, ele fará, provavelmente, uma análise da personalidade do seu alvo, estudando o seu comportamento e verificando se se trata de uma pessoa que pensa nos argumentos apresentados ou age impulsivamente. Isso lhe permitirá adotar a atitude mais "convincente".

Na documentação da referência, são destacados quatro dos elementos constitutivos da persuasão, a saber: o comunicador, a mensagem, a forma de comunicação e a audiência. Vejamos algumas considerações básicas sobre cada um desses elementos:

- o comunicador – ao bom comunicador (comunicador persuasivo) são atribuídas as qualidades da credibilidade, decorrente da sua especialização e fidedignidade, e da atratividade ou simpatia, fruto de atração física ou de similaridade (semelhança como destinatário da mensagem transmitida). Falar rapidamente, com convicção e encarando o "alvo" pode ajudar na persuasão.
- a mensagem – ao conteúdo da mensagem, é atribuído maior ou menor poder de influência quando se associa os aspectos racionalidade e/ou emotividade da mensagem ao tipo de assistência a que ela é dirigida. Myers, citando outros autores, mostra- nos que pessoas instruídas reagem mais aos apelos racionais do que pessoas menos instruídas. Da mesma forma, ainda demonstra que mensagens associadas a bons sentimentos são mais persuasivas. (Myers, 2000)
- a forma de comunicação – com relação a esse ítem, acreditamos que seja importante destacar que é a combinação da complexidade da mensagem com o meio de disseminação que vai estabelecer o grau de persuasão.
- a audiência – é preciso que se tenha em consideração que, de acordo com William Mcguire (citado por Olsson's), são três os determinantes que definem o tipo de plateia a qual nos dirigimos: a idade, o sexo e a inteligência. E cada um deles condiciona, de forma específica, a receptividade e a reação da plateia.

Do que já foi exposto, parece-nos ser possível inferir que a persuasão é resultado dinâmico de uma atividade de comunicação interpessoal e que a capacidade de persuadir pode ser desenvolvida mediante a observância e a adoção de certas técnicas, algumas delas bem definidas pela psicologia social, como as acima enumeradas.

Entretanto, cabe ressaltar que existem muitas outras obras publicadas sobre o assunto, algumas delas de autores de outras áreas do conhecimento, tais como o livro "A Mágica da Persuasão", de Laurie Phun, advogada, mediadora e palestrante, no qual a autora descreve 35 regras para melhorar o processo de comunicação entre pessoas.

Dessas regras destacamos as seguintes:

- enriqueça os elogios:

"Todos temos a mesma necessidade humana básica de sermos apreciados. (...) Quando suas palavras fazem com que alguém se sinta admirado e valorizado, você consegue que essa pessoa imediatamente o admire e valorize". (Puhn, 2005. pág 81)

- transforme as pessoas em parceiros:

"... o importante é saber que é possível conseguir o que se pretende das pessoas sem dar ordens. Como? Usando o poder da persuasão.(...) A persuasão é uma maneira eficaz de conseguir que alguém *queira* fazer algo por você". (Puhn, 2205. pág 101)

- prepare seus argumentos:

"As pessoas precisam ouvir suas razões e provas para compreender as suas pretensões e se convencerem de que você está certo". (Puhn, 2005. pág 129)

- "quem não chora não mama":

"Quando você quiser algo, peça. As pessoas às vezes não sabem o que você quer, só você". (Puhn, 2005. pag 184)

Ao pesquisar a literatura a respeito de comunicação interpessoal, verificamos que podemos entender comunicação como um processo transacional, contínuo e colaborador de troca, transmissão ou transferência de dados, informações e/ou conhecimentos, que se constitui em necessidade básica da humanidade.

O ser humano, por se tratar de um ser social, precisa estabelecer relacionamentos e, para isso, utiliza-se desse processo.

Ora, se a comunicação é uma necessidade do ser humano e a persuasão decorre da capacidade do locutor de usar a comunicação para influenciar ou convencer seus ouvintes, então julgamos oportuno relatar que Adler e Towne (2002) apresentam, como característica de uma comunicação competente, a adaptabilidade (flexibilidade), em outras palavras, o "jogo de cintura" do comunicador, a "circunstancionalidade" e a "relacionalidade".

Esses mesmos autores ressaltam que no processo de comunicação nem sempre o que se transmite é o percebido pelo receptor, e que isso acontece em função do esquema perceptivo desse último. O processo perceptivo sofre influência direta de aspectos fisiológicos, culturais e comportamentais, que frequentemente nos conduzem a erros de percepção.

E são justamente os aspectos culturais e comportamentais que o Engenheiro Social procurará manipular para atingir seu intento de "conduzir" as ações do seu "alvo", a fim de obter livre acesso às informações desejadas.

8 CONCLUSÃO

O estudo do assunto proposto não se esgotou neste artigo, até porque esse nunca foi o nosso objetivo. Nem mesmo chegamos a fazer um estudo aprofundado sobre o tema central, pois, na verdade, cada um dos tópicos desenvolvidos no trabalho poderia ensejar várias pesquisas específicas.

No entanto, mesmo com essa abordagem superficial, baseada em uma revisão bibliográfica reduzida, concluímos o trabalho com a esperança de termos conseguido demonstrar que o tratamento da informação exige uma gestão apropriada, especificamente elaborada e convenientemente dimensionada. Tal cuidado deve-se à necessidade de preservação desse importantíssimo patrimônio organizacional em face das diversas ameaças existentes no mundo moderno, mais do que digitalizado, virtualizado e globalizado por meio da rede mundial de computadores, a Internet.

No cenário mundial, os crimes também foram modernizados, são executados, muitas das vezes, de forma virtual, e são tecnologicamente bastante sofisticados. Mundo onde "hackers", "crackers" e "phreakers" se misturam de forma quase equitativa com vaidade, inocência, ingenuidade, incompetência e despreparo para comporem uma das formas mais eficiente de apropriação indébita, a Engenharia Social.

Esperamos, principalmente, ter conseguido

– este sim era o nosso principal objetivo – demonstrar que, embora em muitas ocasiões os Engenheiros Sociais atuem de forma intuitiva, quando eles agem conscientemente, ou seja, fazendo uso da persuasão e respeitando os princípios básicos da psicologia social aplicados às técnicas de comunicação interpessoal, torna-se quase impossível resistir aos seus ataques. A única providência cabível é treinar e capacitar convenientemente os profissionais para identificar e reagir apropriadamente à investida desses meliantes, assim como às outras diversas ameaças eletrônicas e virtuais desenvolvidas pelos denominados "cibercriminosos".

REFERÊNCIAS

A Bíblia Sagrada. 44. Ed. São Paulo: Edições Paulinas. 1997

Adler, Ronald B; Towne, Neil. *Comunicação Interpessoal*. Rio de janeiro: LTC editora, 2002.

Arima, Kátia. *A Tecnologia do Crime*. Revista Info-Exame, n. 281, p.61-67, jul. 2009.

Assis, Wilson Martins de. *Gestão da Informação nas Organizações*. Belo Horizonte: Autêntica Editora, 2008.

Batista, Emerson de O. *Sistemas de Informação*: o uso consciente da tecnologia para o gerenciamento. São Paulo: Saraiva, 2004.

Braga, Ascenção. *A Gestão da Informação* Disponível em: <http://www.ipv.pt/millenium/19_arq1.htm> . Acesso em 22 jun. 2009.

Caparelli, David; Campadello, Pier. *Templários:* sua origem mística. São Paulo: Madras, 2003.

Castells, Manuel. *A Sociedade em Rede*. São Paulo: Paz e Terra, 2003.

Correia, André. *Segurança: questão de sobrevivência dos negócios*. Dispoível em: <http://www.infoguerra.com.br/infonews/talk/1012557620,12815,.shtml>. Acesso em 23 jun. 2009.

Costa, Jose Carlos Villela da. *A segurança da Informação no Sistema de Comando e Controle do Exército:* situação atual, vulnerabilidades, deficiências e proposta de implementação de novas tecnologias. 2008. 67p. Monografia (trabalho de conclusão de curso de especialização) CPEAEx/ ECEME, Rio de Janeiro.

Machado, André. *Cuidado com a e-perseguição*. Jornal O Globo, Rio de Janeiro. 29 jun. 2009. Caderno Digital, p. 15-17

_____. *Tudo pelo Social*. Jornal O Globo, Rio de Janeiro. 06 jul. 2009. Caderno Digital, p. 12-15

_____. *Cibercriminosos de Olho na Nuvem*. Jornal O Globo, Rio de Janeiro. 20 jul. 2009. Caderno Digital, p. 12-13

Drucker, Peter. *Administrando para o Futuro*: os Anos 90 e a virada do século. São Paulo: Thomson Pioneira, 1998.

Ferreira, Aurélio Buarque de Holanda. *Dicionário da Língua Portuguesa*. Rio de Janeiro. Nova Fronteira, 1999.

Ferreira, Fernando Nicolau Freitas; Araújo, Márcio Tadeu de. *Política de Segurança da Informação: guia prático e implementação*. Rio de Janeiro: Ciência Moderna, 2006.

Fontes, Edison. *Praticando a Segurança da Informação*. Rio de Janeiro: Brasport, 2008.

_____. *Segurança da Informação: o usuário faz a diferença*. São Paulo: Editora Saraiva, 2006.

Junior, Evaldo Tatsch. Artigo *A importância da prática da Engenharia Social*. Disponível em: <http://www.istf.com.br/vb/etica-e-comportamento/13692-importancia-da-

pratica-da-engenharia-social.html>. Acesso em 25 jun. 2009.

Klein, Soeli Claudete. *Engenharia Social na Área da Tecnologia da Informação*. 2004. 63 pág.. Monografia (trabalho de conclusão de curso). Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale. Novo Hamburgo, RS.

Laudon, Kenneth C.; Laudon, Jane Price. *Sistemas de Informação com Internet*. Rio de Janeiro: LTC, 1999.

Laureano, Marcos Aurelio Pchek. *Gestão de Segurança da Informação*. Disponível em: <*www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf*>. *Acesso em 03 jun. 2009.*

Man, John. *A história do Alfabeto: como 26 letras transformaram o mundo ocidental*. Rio de Janeiro: Ediouro, 2002.

Olsson's, Johan. *Persuasion in Practise*. Disponível em: <http://www.geocities.com/TimesSquare/1848/pers.html>. Acesso em 04 ago. 2009.

Myers, David G. *Psicologia Social*. Rio de Janeiro: LTC Editora, 2000.

Mitnick, Kevin D.; Simon, William L. *A Arte de Enganar*. São Paulo: Pearson Education do Brasil, 2003.

Mitnick , Kevin D.; Simon, William L. *A Arte de Invadir*. São Paulo: Pearson Education do Brasil, 2006.

Peixoto, Mário César Pintaudi. *Engenharia Social e Segurança da Informação*. Rio de Janeiro: Brasport, 2006.

Phun, Laurie. *A Mágica da Persuasão*. Rio de Janeiro: Elsevier Editora, 2005.

Sêmola, Marcos. *Gestão da Segurança da Informação*. Rio de Janeiro: Editora Campus, 2003.

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

Silva, Estela. *Artigo Especial sobre Segurança*. Disponível em: <http://www.sit.com.br/SeparataGTI089.htm>. Acesso em 25 jun. 2009.

Stair, Ralph M.; Reynolds, Geroge W. *Princípios de Sistemas de Informação.* Rio de janeiro: LTC, 2002.

Toffler, Alvin. *A Terceira Onda*. Rio de Janeiro: Record, 1980.

(*)O autor é Coronel da Reserva do Exército Brasileiro, Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME). Possui especialização em Análise de Sistemas – Centro de Estudos de Pessoal do Exército (CEP), em 1989; MBA de Gestão Empresarial com ênfase em RH – UFRJ/ 2003/2004; e MBA executivo da FGV, em andamento. (Email: abnersilva@uol.com.br)