A ENGENHARIA SOCIAL E OS DESAFIOS DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

Luís Gustavo Silva Costa [1]

Sarah Cruz [2]

RESUMO

O armazenamento da informação é uma das mais enriquecedoras invenções que o homem conquistou no mundo contemporâneo. Desde que aprendeu a armazenar dados e manuseá-los a fim de sustentar, aprimorar e revolucionar a forma de se enxergar uma gestão, um degrau evolutivo foi alcançado. O objetivo deste artigo é refletir sobre a disseminação da tecnologia em todos os setores da vida cotidiana e procura estudar especialmente as tecnologias da informação, atualmente visadas por pessoas desonestas que, através de crimes e ataques, colocam em risco a credibilidade das mesmas. Nasce, portanto, a necessidade de se proteger os dados, tornando-os inalcançáveis àqueles que não são requisitados no processo. Este artigo discute a revolução tecnológica, os impactos na gestão empresarial e os recentes desafios causados por tamanha mudança, tais como a segurança da informação e a engenharia social. O trabalho pôde explanar de forma teórica o assunto e compreender a forma que a tecnologia funciona atualmente e também as ameaças e desafios que surgem a todo momento.

Palavras chave: Segurança da Informação, Engenharia Social, Gestão Empresarial

1 INTRODUÇÃO

A informação tem se tornado item essencial em qualquer gestão atual e tamanha é sua importância que muitas estratégias giram em torno do bom funcionamento e relacionamento que ela possui dentro da empresa. A importância que a informação adquiriu para as organizações com o passar do tempo levou ao surgimento de um novo modelo de economia, embasada na informação como valor primordial para uma boa administração.

Luís Gustavo Silva Costa, pós-graduando em MBA em Tecnologia da Informação, e-mail: luisgusc@gmail.com
Sarah Cruz - Orientadora. e-mail: pos.artigos@unis.edu.br

Os modelos de gestão têm se revolucionado e junto deles, mudam-se as ferramentas e as maneiras de se enxergar os processos. As informações são tratadas com muito mais cuidado e ordem atualmente, sendo consideradas itens valiosos para um bom gerenciamento.

Assim como a administração torna-se preocupada com a informação, os inimigos encontram nesta dependência uma forma de exploração efetiva. Os gestores preocupam-se cada vez mais com os riscos de possíveis ataques e acesso indevido às informações, colocando em pauta a confiabilidade das mesmas. Faz-se necessário então, não somente um bom manuseamento e asseguração das áreas que envolvem a informação, mas ainda entender e saber se prevenir de ações criminosas envolvendo a tecnologia.

O setor da Tecnologia da Informação (TI) é imensamente mais visado do que anos atrás e este destaque só tende a aumentar cada vez mais. Os profissionais que lidam com a TI precisam estar atualizando-se e evoluindo suas técnicas, práticas e conhecimento geral dos recursos e características da área. É preciso ainda compreender o mercado e suas variabilidades, não perdendo a capacidade de entende-lo e assim tornando-se obsoleto.

O seguinte artigo tem a finalidade de discutir, através de pesquisa bibliográfica, a evolução da segurança da informação e também as ameaças que se desenvolvem juntamente à esta corrente, como a engenharia social. A próxima seção apresenta o referencial teórico utilizado para elaboração do artigo científico.

2 A SEGURANÇA DA INFORMAÇÃO

Segundo Machlup e Mansfield (1983), a informação pode ser caracterizada como o meio necessário para a extração e construção do conhecimento, enquanto a Associação Brasileira de Normas Técnicas (ABNT) (2005) afirma que a informação é tida como um ativo fundamental e, por isso, é preciso que haja uma proteção adequada, uma vez que a própria tecnologia que a criou e possibilitou que ela se incorporasse tão ativamente das revoluções administrativas, tornando-a comunicativa, acessível e rápida, também criou o revés deste aprimoramento, que é o mau uso da tecnologia através ameaças, vulnerabilidades que colocam em risco a informação empresarial.

De acordo com Posthumus e Von Solms (2004), tais vulnerabilidades e ameaças podem prejudicar organizações a níveis estratégicos ou financeiros, o que é um fator a ser evitado ao máximo, já que isso implica diretamente na imagem da empresa. Assim, os mais precavidos e atentos às suas próprias gestões, estabelecerem e passaram a manter estruturas para tratar de problemas relacionados à Segurança da Informação, segundo Eloff e Von Solms (2000).

O termo Segurança da Informação é caracterizado por Beal (2005) como a proteção dos dados de informação contra ameaças à sua integridade, confidencialidade e disponibilidade, o que é semelhante a uma das duas definições apresentadas pela ABNT (2005). Na norma NBR ISO/IEC 27002:2005 da ABNT, Segurança da Informação é definida: como a preservação da confidencialidade, da integridade e da disponibilidade, seus três pilares; e como a proteção da informação contra ameaças para minimizar o risco e garantir a continuidade do negócio, maximizar as oportunidades de negócio e o retorno sobre os investimentos.

> 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, p. 11)

Essas definições compactuam com a finalidade da Segurança da Informação, que, segundo Sêmola (2003), é a proteção dos dados de informação contra indisponibilidade e uso não autorizado, e de acordo com Mandarini (2004), é proteger as informações para que se assegure da continuidade do negócio, minimizando perdas e maximizando o retorno sobre os investimentos.

Segundo Mello (2010), a segurança da informação pode ser caracterizada pela preservação de três fatores:

- Confidencialidade: Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- Integridade: Exatidão, completeza da informação e dos métodos de processamento;
- Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A política de segurança da informação define os limites de um comportamento desejável dentro da organização no que tange à informação. Essa proteção da informação necessita ser direcionada por políticas e procedimentos de Segurança da Informação, ofícios elaborados e aprovados formalmente por uma supervisão capacitada, posteriormente publicados para toda a empresa, fornecedores e clientes da organização. Segundo Siqueira:

> 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, p. 57).

Para a ABNT (2005), uma política deve discorrer acima de diversos aspectos relacionados à Segurança da Informação, incluindo processos, procedimentos e estruturas organizacionais, além dos recursos tecnológicos e da infraestrutura necessários, enquanto Marciano (2006) afirma que estes documentos devem ainda abranger os recursos tecnológicos, a estrutura empresarial, a logística e os processos de RH necessários para proteger as informações.

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003, p. 3).

Em outras palavras, a Segurança da Informação deve não pensar estritamente a respeito dos aspectos tecnológicos de uma empresa, mas também sociais e políticos. Como a Segurança da Informação detém uma grande preocupação com o aspecto social, inclusive para realização de estudos científicos, pensar no homem antes do sistema tecnológico é uma boa forma de se planejar uma adequada defesa e política de tráfico de informações.

2.1 Implementação de políticas de segurança organizacionais e suas vantagens

As políticas de segurança são normas claras que oferecem orientações de comportamento do colaborador a fim de preservar informações, tornando-se um elemento essencial para desenvolver uma gerência segurança e embasando adequadamente para possíveis contra-ataques em ameaças à segurança da empresa. Estas políticas configuram um posto de destaque quanto às medidas para evitar e detectar ataques de engenharia social. Segundo Mitnick e Simon (2003) todos têm desafetos ou inimigos, portanto, em ambientes organizacionais, onde a competição assume caráter de permanência ou exclusão do mercado, é preciso ter a maior atenção possível. Por isso, através de treinamento adequado e campanhas de conscientização, é possível desenvolver e aplicar políticas de segurança, embora seja importante observar que mesmo seguidas à risca por todos os componentes da gestão, é impossível "blindar" a segurança da engenharia social. Por isso, um objetivo ideal seria sempre minimizar o risco até um nível aceitável.

> "A informação é um ativo que, como qualquer outro, importante para os negócios, tem um valor para a organização. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos ao negócio e maximizar o retorno dos investimentos e as oportunidades de negócios". (NBR ISO/IEC 17799:2005, p. 31)

Estabelecer o nível de segurança é prioridade máxima. Ele deve garantir que cada componente da gestão só possa acessar o conteúdo que lhe é permitido; por exemplo um assistente administrativo, o qual deve possuir contato apenas ao conteúdo informativo que lhe diz respeito, impossibilitando-o de acessar uma fonte de dados pertencente a outro departamento que não seja diretamente relacionado com as funções na qual ele desempenha. Para Mitnick e Simon (2003, p.16) a segurança não é um produto, ela é um processo. É comparada como um produto a ser testado; implanta-se e verifica-se a efetividade do sistema na gestão. Tal pensamento é antiquado, pois ignora o fato de que não basta apenas comprar e instalar o sistema. Pelo contrário, ao deixá-lo "rodando", sem supervisão, pode tornar a empresa ainda mais vulnerável do que antes, porque é necessário que haja uma constante e atenta adequação ao sistema.

De acordo com Peixoto (2006, p. 36), a engenharia social está inserida como um dos mais complexos e constantes desafio no âmbito das vulnerabilidades encontradas na gestão da segurança da informação. Sendo assim, uma política de informação agrega benefícios como evitar relapsos que acabem tornando em vazamentos, fraudes, espionagem proveniente de concorrentes, uso indevido, sabotagens são esperados após implementação, tangendo ainda na precaução em diversos outros problemas que venham a prejudicar a empresa de alguma forma.

> De acordo com as pesquisas mais recentes, aproximadamente 53% das empresas brasileiras apontam os funcionários insatisfeitos como a maior ameaça à segurança da informação, 40% delas afirmam ter sido vítimas de algum tipo de invasão, 31% não sabem dizer se sofreram ataques e somente 29% alegam nunca ter sofrido ataques, [...]. Em 22% dos casos de ataque, as organizações não conseguiram detectar as causas e em 85% dos casos não souberam quantificar o prejuízo. (BANNWART, 2001 apud PEIXOTO, 2006, p. 36).

Quando existe segurança da informação, é esperado também que o funcionário aumente sua produtividade e possua mais confiança ao executar suas funções, características alcançadas através de ambiente mais organizado e seguro. Os custos da implementação de sistemas de segurança da informação variam e são flutuantes de acordo com as necessidades organizacionais de cada gestão, necessitando-se uma análise criteriosa para que se escolha alguma iniciativa de proteção empresarial.

Toda empresa, gestão e até mesmo pessoa comum pode ter sua própria política de segurança, visando melhorar a qualidade da confidencialidade das informações que lhe cabem. Para começar, uma boa senha deve priorizar a segurança, o que foi taxado por algumas publicações divulgadas pelo Departamento de Defesa Americano (DoD), em 1985. O documento do DoD esquematizou recomendações que norteiam indivíduos a escolher e cuidar apropriadamente de suas senhas. Feito isso, deu-se origem às seguintes regras (Smith, 2002):

1. Cada senha escolhida deve ser nova e diferente, já que o uso de uma única senha para vários sistemas pode dar aos invasores uma grande vantagem ao interceptar uma só senha;

2. Senhas devem ser memorizadas. Se uma senha é registrada em papel, este deve ser armazenado em local seguro;

3. Senhas devem ser compostas de pelo menos seis caracteres, provavelmente mais, dependendo do tamanho do conjunto de caracteres usado, i.e. se contêm apenas números, números e letras, ou se contêm uma combinção de números, letras e outros caracteres do teclado como, por exemplo, "*", "%", "$", "#", "@", e outros;

4. Senhas devem ser substituídas periodicamente;

5. Senhas devem conter uma mistura de letras (tanto maiúsculas quanto minúsculas), dígitos e caracteres de pontuação.

É preciso ter consciência de que a segurança das informações é uma importante ação da empresa, possibilitando que as informações comerciais permaneçam sendo disponibilizadas àqueles que as necessitam e assim, tudo continue funcionando e não haja prejuízos ou perdas. Também é importante que as normas de segurança deixem claro que cada política precisa ser seguida, caso contrário, os empregados podem enxergá-las como desnecessárias e não respeitá-las.

Segundo Silva (2008), a falta de políticas de segurança da informação em um âmbito organizacional configura como uma falha muito grave, por motivos de vulnerabilidade e também falta de referência, já que o gestor de segurança não terá fundamento ou ponto de partida para instituir práticas estratégicas que visem a melhoria da segurança na empresa. O autor, por fim, destaca os dez principais erros cometidos por uma gestor de segurança em um ambiente organizacional:

1. A falta de políticas;

2. A falta de uma gestão de controle de acesso;

3. A falta de um gestor da informação;

4. Não cumprir os planos de continuidade;

5. Falta de registros das ações realizadas;

6. Cópias de segurança;

7. A falta de um gestor de processo de segurança;

8. A falta de uma gestão de risco;

9. A não existência de um paralelo entre a segurança e o negócio;

10. Funcionário pouco treinado e não conscientizado.

3 A ENGENHARIA SOCIAL

De acordo com Alexandria (2009), o termo engenharia social popularizou-se na década de 90, através de um famoso hacker chamado Kevin Mitnick, utilizador de técnicas para obtenção de dados que lhe auxiliassem em invasões. Sua fama foi tanta, que o jovem americano de dezessete anos tornou-se uma “celebridade” ao invadir o sistema do Comando de Defesa Aérea dos Estados Unidos. As práticas são

provenientes, em grande ocorrência de vezes, de pessoas próximas ao designado alvo e o termo Engenharia Social pode ser tomado como sinônimo de espionagem.

A denominação caracteriza práticas utilizadas no intuito de obter informações sigilosas ou importantes de corporações, sistemas ou pessoas físicas, utilizando-se da confiança da pessoa a fim de enganá-la e assim, corromper o seu sistema de informação (ou a falta dele) ao alcançar acesso indevido ao conteúdo desejado pelo malfeitor. É possível ainda definir engenharia social como a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações. (SILVA, E., 2008). Há ainda a seguinte definição:

> 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. (KONSULTEX, 2004 apud PEIXOTO, 2006, p. 4).

O termo “engenharia” foi delegado a essa prática porque é constituída acerca de informações e táticas de acesso a informações sigilosas de maneira indevida. O termo “social” designa a utilização de pessoas ou grupo de pessoas que possuem acesso a algo que seja desejável. Pode parecer recente, mas estas práticas são muito antigas, provenientes de casos de detetive que desejam obter informações e também por magistrados com o intuito de validar se um confesso dizia a verdade (SANTOS, 2004, p. 93).

De acordo com Wasserman (WASSERMAN; FAUST, 1999, p. 17), hackers, quando munidos de técnicas de engenharia social, apoderam-se de falhas ou características comportamentais específicas e buscam fraquezas sociais, psicológicas ou até mesmo pessoais, sendo as mais utilizadas:

> • Vaidade (pessoal ou profissional): há maior receptividade a avaliação positiva e favorável que coincida com interesses e objetivos pessoais. Assim, a identificação com argumentos concordantes com a avaliação pessoal ou profissional gera aceitação espontânea.
>
> • Autoconfiança: é intrínseca a vontade de se transmitir em diálogos o ato de fazer algo bem (mostrar-se bom em determinado assunto, área ou habilidade), coletivamente ou individualmente, procurando transmitir segurança, conhecimento, saber e eficiência, objetivando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou indivíduo.

> • Formação profissional: é permanente a busca pela valorização da formação e habilidades adquiridas, demonstrando domínio na comunicação, execução ou apresentação, almejando o reconhecimento pessoal inconscientemente em primeiro plano.
>
> • Vontade de ser útil: é bem visto agir com cortesia, bem como ajudar outros quando necessário.
>
> • Busca por novas amizades: é nato sentir-se bem quando elogiado, criando-se um estreitamento afetuoso e a sensação de intimidade, tornando o “alvo” mais vulnerável e aberto a ceder informações.
>
> • Propagação de responsabilidade: o compartilhamento do encargo traz a sensação de conforto, de que não se está sozinho na busca da solução do que foi proposto.
>
> • Persuasão: é possível obter dados específicos de forma indireta, identificando características comportamentais que tornam as pessoas vulneráveis a manipulação através de uma considerável quantidade de técnicas disponíveis a qualquer pessoa que tenha interesse em adquiri-las.

3.1 – O embate entre a organização e técnicas de engenharia social

Sendo a engenharia social uma ferramenta onde exploram-se falhas humanas em organizações físicas ou jurídica, responsáveis pelo sistema de segurança da informação detém poder decisivo parcial ou total ao sistema de segurança da informação, sendo ele virtual ou ainda físico, porém, é preciso considerar que as informações pessoais, não documentadas, conhecimentos e domínios pessoais, não são informações físicas ou virtuais; estas fazem parte de grupo que possui características comportamentais e psicológicas, tendências nas quais a engenharia social passa a ser executada. Dentre as várias formas de furto de informações da engenharia social, em Mitnick (2003) destaca-se:

> [...] Em vez de ficar se descabelando para encontrar uma falha no sistema, o hacker pode largar no banheiro um dispositivo de armazenamento infectado, com o logotipo da empresa e uma etiqueta bem sugestiva: 'Informações Confidenciais. Histórico Salarial 2003'. É provável que alguém o encontre e insira na máquina. (MITNICK, 2003, p. 273)

De acordo com FERREIRA (2009) têm-se os seguintes significados para Engenharia: aplicação de conhecimentos científicos e empíricos e certas habilitações especificam a criação de estruturas, dispositivos e processos para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas (p. 754) e Social: da sociedade ou relativo a ela, sociável (p. 1864).

Um engenheiro social não é uma pessoa formada em engenharia social, já que engenharia social não é uma faculdade e sim um conjunto de técnicas, mas se caracteriza como um sujeito capacitado em diversas áreas, profundamente ou não, que usará tais ciências para obter informações ou dados que sejam, a ele, de alguma forma, necessários. Segundo Magalhães (2004):

> Pesquisa feita pela Symantec com 200 companhias sedadas no Brasil revela que 80% investem até 10% do orçamento total em segurança e 57% dedicam até 5%. O estudo mostra ainda que os vírus e códigos maliciosos seriam a causa de 54% dos problemas digitais enfrentados. Em seguida estariam as vulnerabilidades de software e hardware com 32% e os ataques causados por funcionários 30%. (MAGALHÃES, 2004 apud PEIXOTO, 2006, p. 39).

Quase a totalidade de profissionais que praticam a engenharia social, de forma benéfica ou não, trabalham em grandes corporações ou em empresas de médio porte, visionando o encontro de falhas em sistemas de segurança da informação ou transitar por falhas, a fim de exploração indevida. Em função destas tendências, constantemente existirão brechas no caráter ou comportamento indesejável por parte de colaboradores desatentos, onde a Engenharia Social poderá ser plenamente eficaz. Mitnick (2003) destaca:

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis.(MITNICK; SIMON, 2003, p. 3).

Para Security One (2011) o “ataque” proveniente da engenharia social é provável que ocorra seguido de uma conversa amistosa, online ou em um encontro pessoal casual, ao telefone ou até mesmo através da sedução. O ataque pode ser considerado bem sucedido quando o usuário, desatento, cai em uma destas estratégias e fornece o que o hacker desejava. Dentre os ataques, o Artigonal (2010) pontua as seguintes práticas:

- Contatos telefônicos, em simulações de atendimento ao suporte ou emergências;
- Contato proveniente de e-mail, abordando determinado contexto direcionado à ocupação da vítima e que a faça acreditar que, de alguma forma, ela possa ajudar o solicitante;

- Contato através de redes sociais, simulando conhecido com afinidades com a vítima;
- Uso de telefone público, dificultando a localização do suspeito;
- “Virar o lixo” eletrônico da vítima em busca de informações valiosas;
- Phising, golpe on-line de falsificação, e seus criadores são falsários e ladrões de identidade especializados em tecnologia;
- No computador do atacante, é feita uma varredura do lixo informático, dificultando a exploração do caso;
- Disfarce de colaboradores ou pessoas relacionadas à vítima, camuflando-se e ganhando acesso livre;
- Visita em pessoa, munido ou não de armamento, para obtenção da informação de forma violenta ou não.

Os seres humanos são seres imperfeitos e multifacetados. Além disso, situações de risco modificam seus comportamentos, e, decisões serão fortemente baseadas em confiança e grau de criticidade da situação. Ainda há um método mais avançado de se obter informações ilícitas, denominado engenharia social inversa. É a versão mais ambiciosa da prática, já que o hacker apropria-se falsamente de uma personalidade, geralmente em posição de autoridade, causando nos demais usuários uma falsa confiança, fazendo com que estes peçam-lhe informações. Deste ponto em diante, o hacker pode obter informações cruciais para a empresa, mas este tipo de ataque requer muito preparo e pesquisa para que não levante questionamentos ou desconfiança.

Segundo Granger (2001), há três métodos de ataque de engenharia social inversa. A sabotagem, a qual o hacker causa problemas na rede e oferece ajuda à vítima, que, instigada a resolver o problema, fornece as informações, configurando a propaganda. O hacker então, já apropriado dos dados que queria, conserta a rede, terminando a fase de “ajuda” da engenharia social inversa. Neste momento o trabalho está feito e a vítima só descobrirá que teve suas informações roubadas tarde demais.

Assim, reitera Granger (2001), se faz necessária a criação, regulamentação e supervisão de políticas de segurança, com o objetivo de amenizar riscos e evitar problemas. O maior risco é de os funcionários tornarem-se complacentes e relaxarem na segurança; por isso a importância da insistência.

4 CONSIDERAÇÕES FINAIS

Os desastres e ocorrências infelizes relacionadas à segurança da informação são, em sua grande maioria, causados pela intervenção humana. Empresas que lidam com seus colaboradores e segurança como tópicos alheios entre si estão sujeitas a ataques e indevido acesso às suas informações. Quando uma organização realiza teste de penetração de segurança e mantém sua equipe consciente dos perigos e precauções desejáveis a fim de evitar problemas possuem um índice muito melhor de defesa e segurança de seus dados.

Ao tratar de segurança da informação, é preciso pensar não somente nas ameaças tecnológicas, atualizadas e melhoradas constantemente. É preciso também pensar na engenharia social e os seus males. Quanto mais bem preparados e cientes das políticas de segurança de sua empresa, melhor será o relacionamento do colaborador para com a tecnologia. É fato que torna-se impossível esperar que, sozinha, a tecnologia seja capaz de detectar, batalhar e se prevenir das ameaças, contudo, quando o homem está envolvido nos processos, mais segura estará a empresa e claro, as pessoas que nela trabalham.

Ainda reitera-se a necessidade do contínuo desta pesquisa, até mesmo pelo fato de a tecnologia da informação estar constantemente evoluindo-se e tornando-se mais revolucionária. A discussão proposta neste trabalho viabiliza uma série de outras pesquisas e aprofundamentos que tornariam ainda mais desenvolvido o tema e a problematização acerca do estudo.

ABSTRACT

The storage of inforhmation is one of the most enriching inventions that man has conquered the contemporary world. Since learning storing data and handle them in order to sustain, improve and revolutionize the way of seeing one management, an evolutionary step has been achieved. The objective of this paper is to discuss the spread of technology in all sectors of everyday life and seeks to study especially information technology, currently targeted by dishonest people who, through crimes and attacks, threaten the credibility of these. Born therefore the need to protect the data, making them unattainable to those who are not required in the process. This article discusses the technological revolution, the impact on business management and the recent challenges caused by such a change, such as information security and social engineering. The work could explain theoretically the matter and understand how

the technology actually works and also the threats and challenges that arise at all times.

Keywords: Information Security, Social Engineering, Business Management

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE JUNIOR, Antonio E. de; SANTOS, Ernani M. dos. **Segurança da Informação em Hospitais: A Percepção da Importância de Controles para Gestores e Profissionais de TI**. Revista Gestão & Saúde, v.4, n.2, p. 1-14, 2012.

ALEXANDRIA, João C. S de. **Gestão de Segurança da Informação – Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica**. São Paulo, 2009. 193f. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.

ARTIGONAL. **Desvendando Engenharia Social**. Disponível em: <HTTP//www.artigonal.com/tecnologias/engenharia-social.html>. Acesso em: 20/10/2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005: **Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação**. Rio de Janeiro: ABNT, 2005, 120p.

BEAL, Adriana. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. São Paulo: Atlas, 2005, 180p.

ELOFF, Mariki M.; VON SOLMS, Sebastiaan H. ***Information Security Management: A Hierarchical Framework for Various Approaches. Computers & Security***, v.19, n.3, mar. 2000.

FERREIRA, Fernando Nicolau Freitas . ARAÚJO, Márcio Tadeu de. **Políticas de segurança da informação - Guia prático para elaboração e implementação**. Rio de Janeiro: Ciência Moderna, 2008.

GRANGER, Sarah. ***Social Engineering Fundamentals, Part I: Hacker Tactics***. Disponível em: <http://online.securityfocus.com/infocus/1527>. Acesso em 22/10/2015.

MACHLUP, Fritz; MANSFIELD, Una. ***Semantic Quirks in Studies of Information***. In: MACHLUP, Fritz; MANSFIELD, Una. ***The Study of Information: Interdisciplinary Messages***. New York: John Wiley, 1983, p.641-671.

MANDARINI, Marcos. **Segurança Corporativa Estratégica: Fundamentos**. Barueri: Manole, 2005, 344p.

MARCIANO, José L. P. **Segurança da Informação – uma abordagem social**. Brasília, 2006. 211f. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

MELLO, Luiz B. de B.; VASCONCELLOS, Lais A.; BRAGANÇA, Lívia de R.; MOTTA, Otávio M. **Contribuição para Gestão de Ativos Intangíveis Organizacionais: Proposição de Um Modelo Baseado no Balenced Scorecard**. In: VI Congresso Nacional de Excelência em Gestão – CNEG, 2010, Niterói. Anais... Niterói: CNEG, ago. 2010.

MITNICK, Kevin D.; SIMON, William L. Mitnick – **A Arte de Enganar - Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Makron Books, 2003, 286p.

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

POSTHUMUS, Shaun; VON SOLMS, Rossouw. ***A Framework for the Governance of Information Security***. Computers & Security, v.23, n.8, p.638-646, dez.2004.

SECURITYONE. **Engenharia Social: explorando os elos mais fracos**. Disponível em: <http://securityone.com.br/artigos/resenha_engenharia_social.pdf>. Acesso em: 22/10/2015.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. Rio de Janeiro: Campus, 2003, 184p.

SILVA, Alexandro. **Dez falhas em segurança da informação**. Disponível em:

http://softwarelivre.org/alexos/blog/dez-falhas-em-seguranca-da-informacao. Acessado

em: 20/10/2015.

SIQUEIRA, Marcelo Costa. **Gestão Estratégica de Informação**. Edição: 1. Editora: BRASPORT, 2005. (Disponível em : http://books.google.com.br/books?id=kKChDwKstagC&pg=PA110&dq=seguran%C3

%A7a+da+informa%C3%A7%C3%A3o&as_brr=3&cd=9#v=onepage&q=seguran%C

3%A7a%20da%20informa%C3%A7%C3%A3o&f=false). Acesso em: 21/10/2015

SMITH, R.E. (2002). ***The strong password dilemma. Authentication: From Passwords to Public Keys. Chapter 6***. Addison-Wesley. Tulving, E. e Craik, F. (2000). The Oxford Handbook of Memory. New York. Oxford University Press US.

WASSERMAN, S.; FAUST, K. ***Social Network Analysis: methods and applications***. In: Structural analysis in social the social sciences series. Cambridge: Cambridge University Press, (1994) 1999.