Information Systems and Technology Management 2

Marcos William Kaspchak Machado
(Organizador)

Atena Editora
Ano 2019

Marcos William Kaspchak Machado

(Organizador)

Information Systems and Technology Management 2

Atena Editora
2019

2019 *by Atena Editora*

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira
Diagramação e Edição de Arte: Lorena Prestes e Karine de Lima
Revisão: Os autores

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

I43 Information systems and technology management 2 [recurso eletrônico] / Organizador Marcos William Kaspchak Machado. – Ponta Grossa (PR): Atena Editora, 2019. – (Information Systems and Technology Management; v. 2)

Formato: PDF
Requisitos do sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
ISBN 978-85-7247-202-9
DOI 10.22533/at.ed.029191903

1. Gerenciamento de recursos de informação. 2. Sistemas de informação gerencial. 3. Tecnologia da informação. I. Machado, William Kaspchak. II. Série.

CDD 658.4

Elaborado por Maurício Amormino Júnior – CRB6/2422

APRESENTAÇÃO

A obra denominada "*Information Systems and Technology Management*" contempla dois volumes de publicação da Atena Editora. O volume II apresenta, em seus 26 capítulos, um conjunto de estudos sobre a aplicação da gestão do conhecimento aos processos de gestão organizacional, operacional e de projetos.

As áreas temáticas de gestão organizacional e de projetos mostram a importância da aplicação dos sistemas de informação e gestão do conhecimento na cultura organizacional e no desenvolvimento de novos projetos.

Este volume dedicado à aplicação do conhecimento como diferencial competitivo para inovação em processos produtivos, traz em seus capítulos algumas aplicações práticas de levantamento de dados, gestão da cultura e governança empresarial, além de ferramentas de monitoramento da qualidade da informação.

Aos autores dos capítulos, ficam registrados os agradecimentos do Organizador e da Atena Editora, pela dedicação e empenho sem limites que tornaram realidade esta obra que retrata os recentes avanços científicos do tema.

Por fim, espero que esta obra venha a corroborar no desenvolvimento de novos, e valorosos conhecimentos, e que auxilie os estudantes e pesquisadores na imersão em novas reflexões acerca dos tópicos relevantes na área de gestão do conhecimento e aplicações dos sistemas de informação para formação de ambientes cada vez mais inovadores.

Boa leitura!

Marcos William Kaspchak Machado

SUMÁRIO

CAPÍTULO 17

PEOPLE AND INFORMATION SECURITY: AN INSEPARABLE BOUNDARY

Camila Márcia Silveira Teixeira
Universidade Federal de Minas Gerais, Escola de Ciência da Informação, Belo Horizonte, Minas Gerais.

Jorge Tadeu Neves
Universidade Federal de Minas Gerais, Escola de Ciência da Informação, Belo Horizonte, Minas Gerais.

RESUMO: A informação é um ativo essencial aos negócios organizacionais sendo considerada um diferencial competitivo e estratégico. De acordo com as melhores práticas de segurança da informação é recomendado adotar medidas eficazes de proteção que englobem todo o ciclo de vida da informação (manuseio, transporte e descarte) e seus três atributos principais da informação: confidencialidade, disponibilidade e integridade. Tais medidas são importantes para minimizar os impactos de um ataque até um nível aceitável. Através da arte da engenharia social um usuário pode ser manipulado por um engenheiro social que cria uma conexão com a vítima para obter informações e, consequentemente, tirar proveito de vantagens. Este trabalho tem como objetivo realizar um levantamento bibliográfico e revisão de conceitos a respeito da segurança da informação, com ênfase na parte mais frágil da segurança da informação, a saber, o elemento humano. Constatou-se a importância das medidas de proteção estarem alinhadas com as necessidades organizacionais, englobando tecnologia, processos e pessoas e estarem alinhadas com o negócio organizacional, levando em consideração que não existe segurança absoluta e que o elemento humano representa a maior fragilidade da segurança informacional.

PALAVRAS-CHAVE: segurança da informação, engenharia social, vulnerabilidades, ameaça, persuasão.

ABSTRACT: Information is an essential asset to organizational business and is considered a competitive and strategic advantage. According to the best information security practices is recommended to adopt effective preventive measures covering the entire information life cycle (handling, transportation and disposal) and the three main attributes of information: confidentiality, availability and integrity. These measures are important to minimize the impact of an attack to an acceptable level.

Through the art of social engineering a user could be manipulated by a social engineer, who creates a connection with the victim to get information and take advantages. This study aimed to carry out a literature review and revision of concepts about information security,

with emphasis on the weakest part of the information security.
From this article we could see the importance of the protection measures are aligned with organizational needs, considering technology, processes and people and are aligned with organizational business, taking into account that doesn´t exist absolute security and that the human element is the most fragile of the informational security.
KEYWORDS: information security, social engineering, vulnerability, threat, persuasion.

1 I INTRODUÇÃO

Informação é um ativo[1] essencial para os negócios de uma empresa e conseqüentemente necessita ser adequadamente protegida. Com o aumento da interconectividade no ambiente dos negócios, a informação fica exposta a ameaças, como por exemplo: fraudes eletrônicas, espionagem, sabotagem, vandalismo, desastres naturais, danos causados por código malicioso[2], *hackers* e ataque de negação de serviço, do inglês (DoS) *Denial of Service*[3](RAMOS et al., 2008; HILES, 2007).

É unânime a necessidade que todas as empresas têm de se tornarem mais ágeis, competitivas, modernas, lucrativas e de estarem preparadas para o crescimento. A informação é, portanto, um dos pivôs desta corrida e, como ativo, bem e patrimônio, precisa estar bem guardada como um segredo de negócio (SÊMOLA, 2003).

As redes de computadores em todas as partes do mundo estão sujeitas a desastres capazes de afetar a disponibilidade das informações. Geralmente para atender as solicitações de serviço, as organizações dependem de alguns requisitos tais como: estabelecimento sede, central de contato, *web site*, recursos[4]. Tais requisitos ficam expostos a desastres que podem comprometer os objetivos da empresa, ficando a cargo da empresa protegê-los para assegurar a competitividade no mercado, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem junto ao mercado (RAMOS et al., 2008; HILES, 2007).

Toda organização é suportada por processos que mantêm relação de dependência com ativos físicos, tecnológicos, humanos, que inevitavelmente possuem falhas de segurança.

Estas falhas podem ser potencialmente exploradas por ameaças, que ao obterem sucesso e gerarem um incidente produzirão impactos nos ativos, tais impactos tendem a estenderem-se pelos processos e a atingirem todo o negócio, através, por exemplo, de prejuízos financeiros e de desgaste a imagem organizacional.

Neste contexto, a segurança da informação visa à proteção das informações contra

1 Tudo aquilo que possui valor e, conseqüentemente, demanda proteção para uma organização.
2 Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.
3 Técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.
4 Todos os bens, pessoas, tecnologias (incluindo instalações e equipamentos), suprimentos, informações (seja eletrônica ou não) que uma empresa tem que ter disponível para uso, quando necessário, a fim de operar e cumprir o seu objetivo.

diversas ameaças com o propósito de garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Ela pode ser aplicada em uma organização por meio de planos, políticas[5], procedimentos, processos, funções de software e hardware dentre outros.

Atualmente com o aumento crescente no volume de informações disponíveis e a grande dependência de sistemas para a realização dos negócios, a aplicação dos conceitos de segurança da informação (SI) na organização auxiliará a diminuir a exposição a riscos, prejuízos financeiros, comprometimento da imagem e ações de responsabilidade legal. Neste cenário, o desafio empresarial passa a ser extrair todos os benefícios da informatização e automação sem que os malefícios associados à falta de segurança sejam maximizados, colocando a empresa em um nível de risco inaceitável (ISO/IEC 27002, 2009; SÊMOLA, 2003).

As normas relacionadas à segurança da informação podem ajudar a organização a desenvolver e mapear ações para atingir maturidade na Gestão de Segurança da Informação. Deste modo, é recomendado às organizações que desenvolvam ações alinhadas com as melhores práticas de segurança a fim de evitar interrupções e assegurar a retomada em tempo hábil de suas atividades críticas. Como padrão de mercado, que aborda boas práticas de segurança da informação, encontra-se a norma ISO/IEC 27001 (do inglês *Internacional Organization for Standardization* / *International Electrotechnical Commission*) (RAMOS et al., 2008).

É considerada uma boa prática que a segurança empresarial seja planejada com uma estratégia equilibrada quanto a segurança e a produtividade. Pouca ou nenhuma segurança pode implicar em um ambiente vulnerável, enquanto uma ênfase exagerada em segurança pode onerar demasiadamente a realização dos negócios e inibir o crescimento e a prosperidade da empresa. O desafio é identificar e alcançar um equilíbrio entre segurança e produtividade, com um foco especial no fator humano, considerado como a vulnerabilidade mais significativa para segurança da informação (MITNICK; WILLIAN, 2003).

Conforme (KARLINS; SCHAFER, 2015), existe um verdadeiro mar de oportunidades para buscar e encontrar pessoas que poderiam se tornar amigas ou mesmo parceiras de longo prazo, como: Facebook, Twitter, Instagram, e-mail, Skype, Dropbox, Linkedin, Lync, salas de bate-papo, comunidades, e-mail, blogs, mecanismos de busca, sites de namoro. Cabe aos internautas ficarem vigilantes quanto às informações sensíveis trafegados na rede, visto que terão um vínculo com a identidade do indivíduo pela eternidade, podendo ser utilizadas por um engenheiro social para descobrir informações sobre o indivíduo e tomar decisões sobre como tratá-lo.

A engenharia social é considerada uma arte de obter informações de usuários para angariar vantagens, que emergiu na sociedade como uma ameaça séria, capaz de atacar de forma eficaz um usuário.

5 Intenções e diretrizes globais formalmente expressas pela direção da empresa.

Os indivíduos geralmente não têm consciência do valor das informações que divulgam e compartilham, bem como dos impactos, caso usadas de forma maliciosa. O que agrava as conseqüências de um ataque, visto que normalmente as pessoas não têm conhecimento da extensão das técnicas de engenharia social, têm dificuldade para perceberem que estão sendo atacadas e que podem vir a serem vítimas. Além disso, elas acreditam que são boas para detectarem ataques (HOBEL et al., 2014; KIMPPA et al., 2015).

O crescimento de recursos para facilitar a comunicação, compartilhamento e uso de informações, como por exemplo: políticas de uso do seu dispositivo ou do inglês BYOD (*BringYour Own Device*), ferramentas de comunicação on-line, ferramentas colaborativas, proveu automatização, facilitação de execução de tarefas diárias, eficácia na comunicação, entretanto proveu também insumos que podem ser utilizados para potencializar um ataque. O que é agravado pelo fato dos indivíduos, geralmente publicarem e compartilharem informações, considerando que as interações estabelecidas são confiáveis e preocupando-se pouco com segurança e privacidade (HOBEL et al., 2014).

Vulnerabilidades em recursos de informação são geralmente exploradas para acesso a informações sensíveis. Entretanto, as proteções podem ser reforçadas, mas mesmo assim tais proteções são impotentes quando um usuário é manipulado por um engenheiro social (HOBEL et al., 2014).

Este artigo visa fazer um levantamento bibliográfico e revisão de conceitos a respeito da segurança da informação e da chamada engenharia social, enfatizando o fator humano, considerado como a parte mais frágil da segurança da informação.

2 I REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO (SI)

Conforme Ramos et al. (2008), a SI pode ser definida como um estado no qual os ativos[6] de informação [7]estão livres de perigos e incertezas. Geralmente, dentro de uma organização, está segurança costuma se aplicar a tudo aquilo que possui valor e, conseqüentemente, demanda proteção.

Ramos et al. (2008) também relatam que há muita dificuldade para alcançar a segurança absoluta, pois é muito improvável conseguir endereçar todas as possíveis situações de prejuízo e também há limitações de recursos financeiros, sendo que à medida que os investimentos em segurança vão crescendo, existe um momento em que o recurso gasto é maior que o valor do próprio ativo a ser protegido. A segurança próxima de 100% é uma meta normalmente buscada dentro do meio militar, onde falhas podem custar vidas, ativo de valor imensurável. Para conferir e estabelecer

6 Tudo aquilo que possui valor para uma organização.

7 Ativos que geram, processam, manipulam, transmitem e armazenam informações, além das informações em si.

um tratamento de segurança a uma informação é necessário garantir seus três atributos ou conceitos principais: confidencialidade, integridade e disponibilidade. A confidencialidade é a propriedade da informação de se manter acessível aos agentes autorizados e, ao mesmo tempo, inacessível aos agentes não autorizados. A integridade é a propriedade da informação de se manter sob controle e poder ser alterada por agentes autorizados e, ao mesmo tempo, impedida de sofrer alterações por agentes não autorizados. E a disponibilidade é a propriedade da informação de se manter acessível a agentes autorizados a qualquer momento que se precise dela.

2.2 CICLO DE VIDA DA INFORMAÇÃO

Conforme Sêmola (2003), as fases do ciclo de vida da informação representam os momentos nos quais a informação é submetida ao tratamento, seja pela ação direta de ativos físicos, tecnológicos ou humanos, incluindo os procedimentos associados a cada um deles. São fases críticas, comumente, momentos de exposição ao risco e que, por isso, devem ser diagnosticadas e trabalhadas pela empresa como parte de um desafio único e integrado de gerenciamento. Segue descrição sucinta das fases:

- Manuseio: Momento em que a informação é criada e manipulada;
- Armazenamento: Momento em que a informação é armazenada;
- Transporte: Momento em que a informação é transportada;
- Descarte: Momento em que a informação é descartada.

O referido autor faz uma analogia entre as fases do ciclo de vida da informação com os elos de uma corrente. Cada fase do ciclo de vida deve resistir à força contrária de ameaças, tornando-se peças igualmente importantes para o todo; a fase mais ineficaz pode comprometer a eficácia da proteção de todo o ciclo de vida. Um comportamento semelhante é identificado em uma corrente; o elo mais fraco poderá comprometer a eficácia da proteção da corrente.

O poder de proteção de uma corrente está diretamente associado ao poder de resistência do seu elo mais fraco, da mesma forma o poder de proteção de uma informação está diretamente associado ao poder de resiliência a ameaças da sua fase mais ineficaz.

2.3 COMUNICAÇÃO

Conforme Ramos et. al. (2008), a comunicação engloba o processo para estabelecê-la, bem como o universo interior tanto de quem emite a mensagem como de quem a recebe, podendo ser realizada através do olhar, pelo jeito de vestir, escrever

ou falar.

O emissor é quem envia a mensagem; o canal é o meio pelo qual ela é enviada; a mensagem é a informação que se transmite; e o receptor é aquele que a recebe. Os ruídos são todas as interferências que podem existir entre um extremo e outro e que podem prejudicar a compreensão.

Em um grupo social ou profissional o relacionamento se constrói pelos seus agentes, a partir de suas realidades, referencias e objetivos. Os laços de amizade, de simpatia ou antipatia podem unir ou afastar as pessoas, estes são influenciados por fatores pessoais que estão sujeitos a coflitos.

2.4 ANÁLISE DE COMPONENTES ESTRUTURAIS

Conforme Ramos et. al (2008) a Segurança da Informação está diretamente ligada à compreensão do contexto, seu significado e sua importância.

A complexidade do mundo interior individual está diretamente relacionada com aspectos individuais tais que são influenciados por aspectos do universo social.

2.5 COMPONENTES ESTRUTURAIS

Conforme Ramos et al (2008) existem quatro componentes principais, o sistema bio-psicosocial, cultural, ecológico e histórico.

2.5.1 SISTEMA BIO-PSICOSOCIAL

Todos os profissionais da organização são responsáveis pela segurança. Contudo, a abrangência e importância dessas responsabilidades podem variar conforme o papel que o profissional exerce na organização.

2.5.2 SISTEMA CULTURAL

Cultura pode ser definida como o conjunto de características humanas que não são inatas, e que se criam e se preservam ou aprimoram através da comunicação e cooperação entre indivíduos em sociedade.

2.5.3 SISTEMA ECOLÓGICO

Fatores externos as questões de trabalho interferem no relacionamento dos funcionários. Estados de ânimo tais como estresse, podem ser nocivos para segurança da informação organizacional.

2.5.4 SISTEMA HISTÓRICO

Quanto ao sistema histórico é importante o entendimento sobre como a organização “pensa e age”, como ela protegeu e protege as suas informações, como os processos evoluíram, se evoluíram e com base em quê.

2.6 ENGENHARIA SOCIAL

De acordo com CERT.br (2012) a engenharia social é uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações.

Conforme (MITNICK; WILLIAM, 2003), geralmente não é simples obter informações sigilosas de instituições de nichos tais como bancário, comercial, contudo as fragilidades dos usuários podem ser facilitadores para obtenção destas informações. Através de técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram persuadir as potenciais vítimas a fornecerem informações ou a realizarem ações.

A engenharia social é uma técnica que utiliza a influência e a persuasão ou manipulação para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, através desta técnica o engenheiro social pode aproveitar-se das pessoas para alcançar os seus objetivos. Para facilitar o alcance dos objetivos ele apresentara um comportamento favorável ao aumento da probabilidade de que ele e a vítima sejam atraídos um pelo outro e experimentem um resultado positivo quando interagirem.

De acordo com (KARLINS; SCHAFER, 2015) as “Leis da Atração” são ferramentas que melhoram a eficácia de uma relação, podendo ser utilizadas por um engenheiro social para moldar relações humanas. Segue lista das leis da atração:

1. A Lei da Semelhança (“Algo em Comum”): pessoas que compartilham as mesmas perspectivas, princípios, crenças, atitudes e atividades tendem a desenvolver relações próximas e reforçarem umas às outras.

2. Farinha do Mesmo Saco: semelhanças conectam as pessoas. Encontrar coisas em comum rapidamente estabelece uma conexão e um ambiente fértil para desenvolver amizades.

3. A Lei da Atribuição Equivocada: quando as pessoas se sentem bem consigo mesmas e não atribuem a sensação boa a uma causa específica, tendem a associar a causa com quem está fisicamente mais perto.

4. A Lei da Curiosidade: quando alguém se comporta de um jeito que produz curiosidade em outra pessoa, isso aumenta significativamente as chances de que ela queira interagir com a outra pessoa numa tentativa de satisfazer essa curiosidade.

5. A Lei da Reciprocidade: as normas sociais ditam que se alguém lhe dá algo ou faz um favor para você, pequeno ou grande, então você fica predisposto a retribuir o gesto.

6. A Lei da Revelação Prévia: indivíduos que revelam mais informações pessoais possuem mais chances de receber em troca o mesmo nível de informação, a revelação prévia promove a atração.

É comum que os engenheiros sociais retratem o máximo de normalidade possível no contato, conhecimento da terminologia interna da organização, interesses comuns aos da vítima, remoção de barreiras e obstáculos, a fim de não levantarem suspeitas e criarem uma conexão com a vítima, tal conexão constrói uma ponte psicológica entre os indivíduos e abre caminho para que vários níveis de amizade se desenvolvam, facilitando a conquista da confiança da vítima e a obtenção de informações. Situações e estados do ambiente ou das pessoas, tais como pressão para atender demandas, escassez de tempo, estado emocional, fadiga mental, falta de conhecimento, representam um fator favorável ao atacante, visto que estes podem distrair a vítima, que pode utilizar um atalho mental para resolução das demandas sem analisar cuidadosamente as informações.

O cientista mais respeitado do mundo no século XX, Albert Einstein, afirmou: “Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro”. Os autores (MITNICK; WILLIAM, 2003) ressalvam que os ataques da engenharia social podem ter sucesso quando as pessoas são estúpidas (devido à, por exemplo: credulidade, a inocência ou a ignorância) ou, em geral, apenas desconhecem as boas práticas de segurança.

Os engenheiros sociais utilizam de traços sociais favoráveis para estabelecer a afinidade e a confiança (como por exemplo: simpatia, educação, gentileza, charme), eles têm habilidade em lidar com as pessoas, intimidá-las, manipulá-las, estimulando emoções tais como medo, agitação ou culpa para obterem as informações que almejam. A intimidação pode criar o medo de ser punido e influenciar as pessoas para que cooperem. Pode também criar o medo de uma situação embaraçosa ou de ser desqualificado para uma próxima promoção.

A manipulação tem sido estudada pelos cientistas há pelo menos 60 anos. Robert B. Cialdini[8], ao escrever para a revista *Scientific American* (edição de fevereiro de 2001), resumiu a sua pesquisa apresentando “seis tendências básicas da natureza humana”, as quais estão envolvidas em uma tentativa de obter o consentimento para uma solicitação, estas podem ser utilizadas pelos engenheiros sociais para suas tentativas de manipulação. Segue relação a seguir:

- Autoridade: As pessoas têm a tendência de atender a uma solicitação que é

8 Psicólogo social, professor, escritor e empresário dentre os mais respeitados nos estudos da persuasão.

feita por uma pessoa com autoridade.

- Afabilidade: As pessoas têm a tendência de atender uma pessoa que faz uma solicitação quando ela conseguiu se fazer passar por alguém agradável ou com interesses, crenças, atitudes semelhantes.
- Reciprocidade: As pessoas podem atender automaticamente a uma solicitação quando recebem ou têm a promessa de receber algo de valor.
- Consistência: As pessoas têm tendência de atender após fazer um comprometimento público ou adotar uma causa.
- Validação social: As pessoas tendem a cooperar quando isso parece estar de acordo com aquilo que as outras pessoas estão fazendo.
- Escassez: As pessoas têm a tendência de cooperar quando acreditam que o objetivo procurado está em falta e que outras pessoas estão competindo por ele.

Os autores (MITNICK; WILLIAM, 2003) recomendam que as organizações utilizem as etapas a seguir para protegerem-se contra a divulgação de informações aparentemente inofensivas:

- O departamento de segurança da informação precisa realizar treinamentos de conscientização, no qual deve detalhar os métodos de ataque utilizados pelos engenheiros sociais;
- Cada um dos empregados precisa ter consciência que a fala de um interlocutor ter conhecimento dos procedimentos da empresa, da linguagem e dos identificadores internos não dá de maneira nenhuma a forma ou a autenticação para o solicitante, nem o autoriza a ter a necessidade de saber as informações;
- Cada organização tem a responsabilidade de determinar o método adequado de autenticação a ser usado quando os empregados interagem com as pessoas que eles não conhecem pessoalmente ou pelo telefone;
- As pessoas que têm a responsabilidade e o papel de criar uma política de classificação de dados devem examinar os tipos de detalhes que parecem inofensivos e podem levar a informações sigilosas;
- O simples conhecimento da terminologia interna da organização pode fazer com que um engenheiro social pareça assumir autoridade e conhecimento;
- Implementar uma política que proíbe a divulgação dos números internos dos funcionários, contratados, consultores e temporários para as pessoas que não são da empresa;
- Desenvolver um procedimento passo a passo para identificar positivamente se um interlocutor que está pedindo os números de telefone é de fato um empregado;
- Cada empresa precisa ter uma política escrita e bem comunicada sobre a divulgação de informações ao públicas;

- Informações, tais como número de empregado, por si só, não devem ser usadas como nenhum meio de autenticação. Todo empregado deve ser treinado para verificar não apenas a identidade do solicitante, como também a necessidade que o requisitante tem de saber da informação;
- No treinamento de segurança, deve-se ensinar essa abordagem aos funcionários: sempre que um estranho pedir um favor, saiba primeiro como negar educadamente até que a solicitação possa ser verificada;
- O treinamento de segurança precisa ser aplicado a todos que trabalham na empresa.

Os autores (MITNICK; WILLIAM, 2003) afirmam que os ataques de engenharia social geralmente têm o mesmo elemento comum: a fraude. A vítima é levada a acreditar que o atacante é um colega ou alguma outra pessoa que está autorizada a acessar informações confidenciais ou que está autorizada a dar a vítima instruções que envolvam a tomada de ações com um computador ou com um equipamento relacionado com o computador.

A maioria dos ataques poderia ser evitada se a vítima seguisse estas etapas quando um indivíduo o solicitasse informações:

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

2.7 EDUCAÇÃO E CONSCIENTIZAÇÃO

Conforme (MITNICK; WILLIAM, 2003), a aprendizagem implica em mudança de hábitos (comportamentos). Segundo Aristóteles, o hábito é de importância básica para a moralidade. Pode-se tratar a habituação distinguindo-a em adaptativa e estabilizadora. Entende-se por adaptativa quando um indivíduo se acomoda a determinadas circunstâncias ao ponto que a ausência delas se fará sentir como um transtorno, e por estabilizadora quando o indivíduo estabiliza em si uma atitude determinada de tal como que fique preferida e conservada.

Práticas de conscientização em segurança da informação são consideradas um processo de aprendizagem, que implica em mudança de hábitos. Em tais práticas é importante atenção especial quanto à forma como o conhecimento será disseminado; é conveniente educar pela compreensão das idéias e fatos e não coagir ou trabalhar o medo, visto que a coação e o medo podem desencadear comportamentos ofensivos a segurança da informação.

Conforme a ISO/IEC 27001 (2009) o treinamento para aumentar a conscientização visa permitir que as pessoas reconheçam os problemas e incidentes de segurança da

informação e respondam de acordo com as necessidades do seu trabalho.

Um Plano de Conscientização em Segurança (PCS) tem como propósito focar a conscientização coletiva da corporação a respeito dos problemas de segurança, visando influenciar as pessoas para que elas mudem seu comportamento e suas atitudes motivando cada empregado a querer entrar no programa e fazer a sua parte para proteger os ativos de informação da organização.

A tecnologia pode ser utilizada em prol de dificultar os ataques de engenharia social, retirando as pessoas do processo de tomada de decisão, entretanto apenas a tecnologia não previne totalmente um ataque de engenharia social. O meio verdadeiramente mais efetivo de amenizar a ameaça da engenharia social é realizar constantemente práticas de conscientização para a população organizacional, aliada com políticas de segurança eficazes, que definam as principais regras para o comportamento de todos os profissionais. Quanto mais bem instruídos em segurança da informação estiverem os profissionais de uma organização, mais atentos estarão ao assédio de um engenheiro social e uma melhor resposta eles serão capazes de elaborar e transmitir em um ataque. Contudo, é recomendado avaliação constante quanto aos estados de ânimo, necessidades e interesses da população organizacional, (a análise de clima [9]pode ser utilizada como um recurso facilitador para este propósito) a fim de precaver que a população organizacional estará preparada adequadamente a um ataque de um engenheiro social, que possa vir a ocorrer a qualquer momento.

2.8 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A ISO/IEC 27001 (2009) define que a política de segurança da informação prove uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. A norma recomenda que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

3 I CONCLUSÕES E CONSIDERAÇÕES FINAIS

A informação é um ativo, bem e patrimônio de suma importância para prosperidade dos negócios organizacionais. Este ativo provê um diferencial de competitividade, agilidade, modernidade, lucratividade, expansibilidade e de imagem. Portanto, é uma boa prática as organizações planejarem estratégias de proteção informacional, equilibradas quanto a segurança e produtividade, englobando todo o ciclo de vida da informação e alinhadas com as melhores práticas de segurança do mercado. É

9 Ferramenta que visa proporcionar a análise da organização com o seu ambiente, bem como o conjunto de condições que caracterizam o estado de satisfação e ou insatisfação dos colaboradores profissionais na empresa e das demais pessoas que com eles interagem.

importante que todas as fases do ciclo de vida da informação (manuseio, transporte e descarte) sejam providas de proteções eficazes, uma vez que uma falha na proteção de uma destas fases pode comprometer a segurança de todo o ciclo de vida da informação.

Nas estratégias de proteção de informação é importante que sejam atendidos os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. Também é importante que seja considerado o fator humano, principalmente quanto ao universo social das populações do contexto organizacional, visto que este fator representa a vulnerabilidade mais significativa para segurança da informação.

É de grande valia que um indivíduo ao estabelecer um processo de comunicação leve em consideração as boas práticas de comunicação segura: conhecer a identidade do receptor, conhecer a identidade do emissor, identificar se o receptor tem autorização de acesso as informações e necessidade de conhecimento das informações, o canal de comunicação e os ruídos na comunicação.

Estas boas práticas de comunicação segura são importantes para evitar e minimizar impactos de ataques de engenharia social. Um engenheiro social com acesso a informações e juntamente com habilidades, técnicas e ferramentas, pode criar uma ponte psicológica com a vítima e explorar vulnerabilidades humanas, visando a conquista da confiança da vítima para aplicar golpes, ludibriar ou obter informações sigilosas e importantes, acarretando impactos inestimáveis.

Todos os profissionais de uma organização são responsáveis pela segurança das informações organizacionais. O sucesso de um ataque de engenharia social pode ser reduzido por meio da implantação de um conjunto de medidas de proteção: plano de conscientização em segurança da informação, políticas de segurança, tecnologias de proteção e estabelecimento de práticas contra divulgação de informações aparentemente inofensivas. Se cada profissional atuar como um indivíduo consciente quanto a segurança da informação e a alta direção praticar, apoiar e prover suporte a gestão de segurança da informação, provavelmente a aculturação da segurança será mais eficiente e possivelmente a integridade, disponibilidade e a confidencialidade de informações sensíveis serão mais bem preservadas de potenciais ameaças, tais como um engenheiro social.

É relevante que recursos para proteção dos ativos estejam alinhados com as necessidades organizacionais. Adquirir proteções que provêm mais que o necessário, acarreta gastos desnecessários, podendo extrapolar o valor do próprio ativo e inviabilizar a aquisição da proteção e ou prover funcionalidades que não são essenciais ou necessárias, por outro lado proteções que provêm menos que o necessário podem deixar o ativo vulnerável a exploração de ameaças, podendo acarretar uma série de prejuízos, como por exemplo, financeiro e depreciação da marca. Para definição das proteções dos ativos é importante considerar tecnologia, processos e pessoas, estando todos estes alinhados com negócio da organização e levando em consideração que não existe segurança absoluta.

Com a era da informação e com os avanços tecnológicos, os recursos de tecnologia para proteção de informações apresentam soluções cada vez mais eficientes, entretanto somente a tecnologia não é suficiente para proteção de informações sensíveis. Tais recursos dificultam que uma ameaça tenha êxito ao explorar uma vulnerabilidade. É importante considerar um conjunto de proteções relacionadas a tecnologias, processos e pessoas. Vale uma consideração e reflexão a respeito de uma hipermensuração da segurança, que pode dependendo do nível vir a afetar valores individuais; até que ponto a intensificação da proteção da informação, além do necessário, pode vir a desproteger valores e esferas individuais que também devem ser protegidas.

REFERÊNCIAS

Affonso, C.; Alevate, W.;Andrucioli, A.; Bastos, A.; Blum, R. O.; Marinho, Z.; Pinto, E.; Poggi, E.; Ramos, A.; e. ***Security Officer* - 1: Guia Oficial para Formação de Gestores em Segurança da Informação**. Zouk: Porto Alegre, 2008. 351p.

Comitê Gestor da Internet no Brasil. **Cartilha de Segurança para a internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 142p.

Gestão de Crises e Continuidade dos Negócios. **Gestão de Continuidade dos Negócios**. Disponível em: http://www.gcnbrasil.com/index.php?option=com_content&view=section&id=5&Itemid=54. Acessoem: outubro. 2015.

Hiles, Andrew. **The Definitive Handbook of Business Continuity Management**.Inglaterra: John Wiley and Sons Ltd, 2007. 668p.

Hobel, H.; Huber, M.; Krombholz, K.; Weippl, E. Advanced social engineering attacks.**Journal of Information Security and Applications**, Elsevier, Vienna, Austria, n.22, 24 out. 2014.

International Organization for Standardization; International Electrotechnical Commission.**ISO/IEC 27001 - Information technology - Security techniques - Information security management system – Requeriments**. Berlin: ISO/IEC, 2009. 25p.

International Organization for Standardization; International Electrotechnical Commission. **ISO/IEC 27002 - Information technology - Security techniques – Code of practice for information security management**. Berlin: ISO/IEC, 2010. 129p.

Karlins, M.; Schafer, J. **Manual de Persuasão do FBI**. Universo dos Livros: São Paulo, 2015. 274p.

Kimppa, K.K.; Malan, M.M; Mounton, F.; Venter, S. H. Necessity for ethics in social engineering research.**Computer & Security**, Elsevier, Indiana, USA, n. 55, 9 set. 2015.

Michaelis. **Michaelis Moderno Dicionário da Língua Portuguesa**. Melhoramentos. Disponível em: <http://michaelis.uol.com.br/>.Acesso em: 05 dez. 2015.

Mitnick D. Kevin; Simon L. William.**A Arte de Enganar. Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. PerasonEducation: São Paulo, 2003. 588p.

Sêmola, M. **Gest**ão da Segurança da Informação: Uma Visão E**xecutiva**. Campus Elsevier: Rio de Janeiro, 2003. 154p.

SOBRE O ORGANIZADOR

Marcos William Kaspchak Machado - Professor na Unopar de Ponta Grossa (Paraná). Graduado em Administração - Habilitação Comércio Exterior pela Universidade Estadual de Ponta Grossa. Especializado em Gestão industrial na linha de pesquisa em Produção e Manutenção. Doutorando e Mestre em Engenharia de Produção pela Universidade Tecnológica Federal do Paraná, com linha de pesquisa em Redes de Empresas e Engenharia Organizacional. Possui experiência na área de Administração de Projetos e análise de custos em empresas da região de Ponta Grossa (Paraná). Fundador e consultor da MWM Soluções 3D, especializado na elaboração de estudos de viabilidade de projetos e inovação.

Agência Brasileira do ISBN
ISBN 978-85-7247-202-9