V SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317 - 8302

Pessoas e Segurança: Um elo inseparável na esfera informacional

CAMILA MÁRCIA SILVEIRA TEIXEIRA
UFMG-ECI
camila.s8t@gmail.com

JORGE TADEU DE RAMOS NEVES
Fundação Pedro Leopoldo (FPL)
jtrneves@gmail.com

V SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317 - 8302

PESSOAS E SEGURANÇA: UM ELO INSEPARÁVEL NA ESFERA INFORMACIONAL

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, armazenamento, 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 lifecycle (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 social engineer, who creates a connection with the victim to get information and therefore take advantages, could manipulate a user. 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.

ISSN: 2317 - 8302

1. Introdução

Informação é um ativo[1] essencial para os negócios de uma empresa e consequentemente 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* (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[3]. 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 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[4], 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).

---

[1] Tudo aquilo que possui valor e, consequentemente, demanda proteção para uma organização.

[2] Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

[3] 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.

[4] Intenções e diretrizes globais formalmente expressas pela direção da empresa.

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. 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 consequências 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 (*Bring Your 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. Referencial Teórico

2.1 Segurança da Informação (SI)

ISSN: 2317 - 8302

Aquilo que se procura proteger está em todo lugar, distribuído por todos os perímetros físicos e lógicos da empresa, sendo enviado e recebido por diversos meios, representado ora por matérias que se pode tocar, ora por conhecimentos e experiências, mantidos pela mente humana que, de alguma forma, ainda não foram materializados, ou ainda, por símbolos binários que circulam por redes de computadores e são processados por sistemas. As empresas que almejam um estado seguro buscam cercar-se de mecanismos que preservem o conhecimento que detêm e que lhes garantam tranquilidade, obtida pela não exposição ao perigo exagerado ou simplesmente por estarem livres dele (Sêmola, 2003).

Conforme Ramos et al. (2008), a SI pode ser definida como um estado no qual os ativos[5] de informação [6]estão livres de perigos e incertezas. Geralmente, dentro de uma organização, está segurança costuma se aplicar a tudo aquilo que possui valor e, consequentemente, 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 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. A Figura 1 ilustra a pirâmide da Segurança da Informação, composta pelos três atributos neste parágrafo citados.

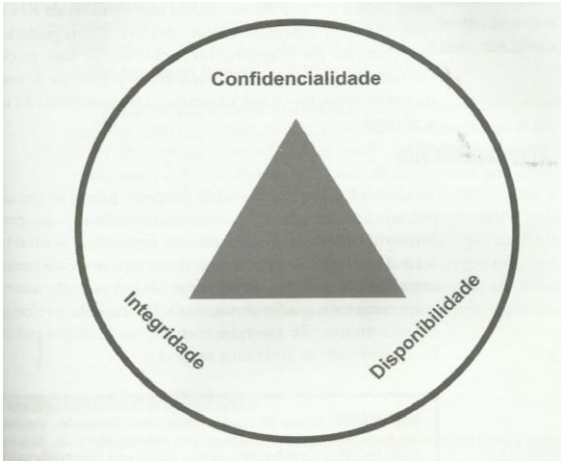

Figura 1: Pirâmide ou tríade da Segurança da Informação.
Fonte: (Ramos et al., 2008).

Entre as décadas de 1970 e 1980, na época dos *mainframes*, enquanto a informática fazia parte da retaguarda dos negócios, os aspectos de segurança tinham como foco principal a confidencialidade dos dados. Nas décadas de 1980 e 1990, com o surgimento dos ambientes de rede, os aspectos de segurança tinham como foco principal a confidencialidade e

[5] Tudo aquilo que possui valor para uma organização.

[6] Ativos que geram, processam, manipulam, transmitem e armazenam informações, além das informações em si.

ISSN: 2317 - 8302

integridade dos dados e informações. Já entre as décadas de 1980 e 1990, os aspectos de segurança tinham como foco principal a confidencialidade, integridade e disponibilidade dos dados, informação e conhecimento. Nesta época a informática passou a fazer parte direta dos negócios, e a proteção passou a priorizar o capital intelectual. Uma análise simplificada deste cenário pode ser visto na Figura 2.

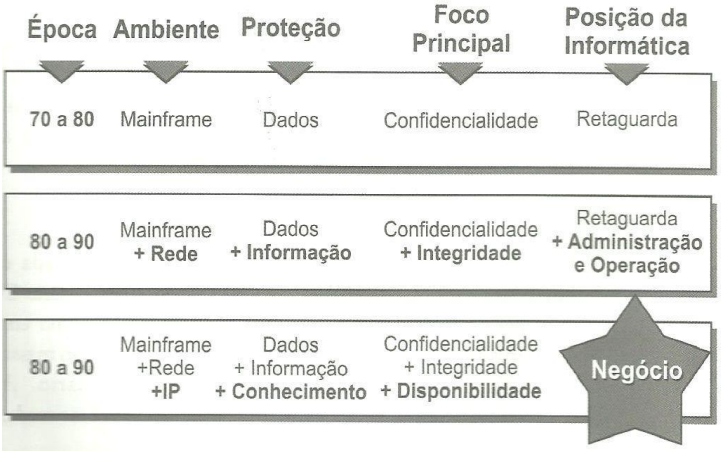

Figura 2: Evolução do cenário da Segurança da Informação.
Fonte: (Ramos et al., 2008).

A partir do século XXI, a segurança da informação tornou-se mais importante para o sucesso empresarial, transcendendo o limite da produtividade e da funcionalidade. Como exemplo de acontecimento que aumentou a importância da segurança nesta época pode-se citar o ataque do vírus "*I Love You*".
Conforme a ISO/IEC 27001 (2009), para se atingir o sucesso na implementação da segurança da informação em uma organização deve-se levar em consideração os seguintes fatores:

- Política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;
- Uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;
- Comprometimento e apoio visível de todos os níveis gerenciais;
- Um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;
- Divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;
- Distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;
- Provisão de recursos financeiros para as atividades da gestão de segurança da informação;
- Provisão de conscientização, treinamento e educação adequados;
- Estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;
- Implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

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. A Figura 3 ilustra a interação entre as fases sob uma ótica da segurança da informação.

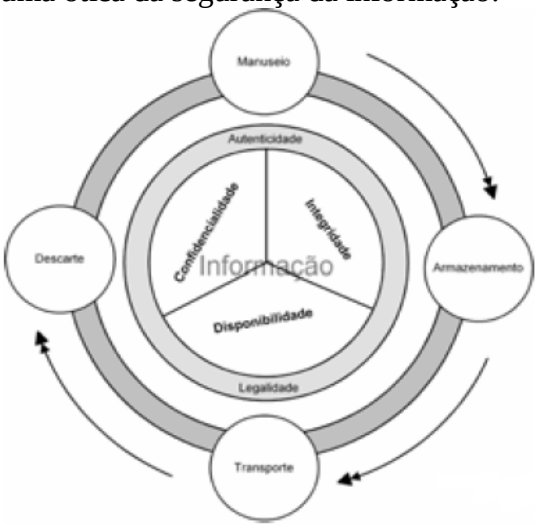

Figura 3: Quatro momentos do ciclo de vida da informação, considerando os conceitos básicos de segurança e os aspectos complementares.
Fonte: Figura retirada de (Sêmola. 2003).

2.3 Ameaça e Incidente

Conforme Sêmola (2003), ameaça é uma atitude ou dispositivo com potencialidade para explorar e provocar danos à segurança da informação, atingindo um ou mais de seus atributos: confidencialidade, integridade, disponibilidade.

ISSN: 2317 - 8302

Para Ramos et al. (2008), ameaças são eventos ou ações que tem potencial de causar algum tipo de dano aos ativos. Quando uma ameaça se concretiza, ela recebe o nome de incidente (situação que pode representar ou levar a uma interrupção de negócios, perdas, emergências ou crises).

2.4 Vulnerabilidade

A vulnerabilidade é uma evidência ou fragilidade que eleva o grau de exposição dos ativos que sustentam o negócio e aumenta a probabilidade de que uma investida de ameaça tenha sucesso (SÊMOLA, 2003).
Para Ramos et al. (2008) as vulnerabilidades criam situações que podem ser exploradas por uma ameaça, acarretando prejuízos. Elas podem ser causadas por várias circunstâncias, mas, no geral, podem ser classificadas como a ausência de um mecanismo de proteção ou uma falha de funcionamento em um mecanismo de controle existente; como por exemplo, ausência de mecanismo de detecção de incêndio, uma falha em um mecanismo de controle de acesso, a ausência de um procedimento de troca periódica de senhas.

2.5 Impacto

No contexto da Segurança da Informação, pode ser definido como o resultado da ação bem-sucedida de uma ameaça ao explorar uma vulnerabilidade de um ativo e atingir, assim, um ou mais atributos da pirâmide da Segurança da Informação (SÊMOLA, 2003).

2.6 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. A Figura 4 exibe os elementos envolvidos no processo de comunicação, conforme:

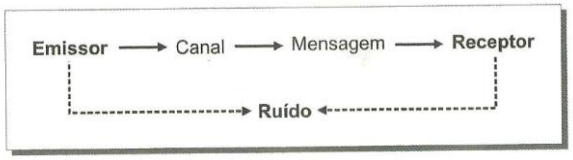

Figura 4: Elementos básicos do processo de comunicação.
Fonte: Figura retirada de (Ramos et al., 2008).

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. Exemplos de ruídos: aspectos emocionais, desconforto interno ou externo. De acordo com o autor existem três tipos de comunicação:

- Comunicação não verbal: simbólica e sonora;
- Comunicação oral: códigos que expressam sensações e sentimentos;
- Comunicação escrita: representação gráfica, como os desenhos e a escrita propriamente dita.

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 tais como:

capacidade intelectual, cultura, aspirações, interesses, temperamento e caráter e estão sujeitos a conflitos, tais como: interesses, valores, sentimentos e emoções. Segundo Ramos et al. (2008), algumas questões humanas interferem na comunicação, conforme descrito a seguir:

- Soberba: manifestação arrogante de um orgulho às vezes ilegítimo, excessivo;
- Inveja: desejo violento de possuir o bem alheio; desgosto ou pesar pelo bem ou pela felicidade de outrem;
- Insegurança: falta de segurança em si próprio, em seus conhecimentos e experiências;
- Medo: sentimento de grande inquietação ante a noção de um perigo real ou imaginário, de uma ameaça, temor, pavor;
- Mentira: impostura, fraude, falsidade. Engano dos sentimentos ou do espírito; erro, ilusão, ideia, opinião, doutrina ou juízo falso;
- Depressão: abatimento moral;
- Vaidade: desejo imoderado de atrair admiração ou homenagens;
- Avareza: apego exagerado ao dinheiro, falta de generosidade, mesquinhez;
- Cobiça: desejo veemente de alguma coisa. Avidez. Ambição desmedida de riquezas;
- Ira: cólera, raiva, indignação. Desejo de vingança.
- Luxúria: lascívia, sensualidade, corrupção de costumes;
- Preguiça: pouca disposição para o trabalho, demora ou lentidão em fazer qualquer coisa; moleza. Negligência, indolência;
- Entusiasmo: veemência, vigor no falar e escrever. Exaltação criadora;
- Decepção: desilusão; desengano; desapontamento. Surpresa desagradável, contrariedade.

Quando um indivíduo quer obter uma informação de outrem utilizando a engenharia social, geralmente busca informações a respeito da vítima tais como: caráter, personalidade, valores, vulnerabilidades, estas serão úteis para o estabelecimento de uma comunicação que lhe permita obter o que quer explorando as fraquezas de um dos ativos humanos da organização. Ramos et. al. (2008) recomendam para proteção das informações de uma comunicação:

- Usar códigos conhecidos;
- Usar meios adequados aos tipos de mensagens e usuários;
- Adotar estilo simples e claro;
- Respeitar o interlocutor, não super ou subestimá-lo;
- Respeitar a cultura organizacional e a do país;
- Evitar “ruídos” nos processos.

2.7 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. O universo humano (que inclui questões sócio familiar, de nutrição, saúde, economia, religiosidade, lazer, segurança, educação, justiça, política, integração social) de uma organização pode ser analisado como um todo ou por perímetros pré-estabelecidos, podendo ser definidos conforme o contexto situacional, como, por exemplo, nos departamentos. A Figura 5 exibe o universo-social e os aspectos a ele relacionados.

ISSN: 2317 - 8302

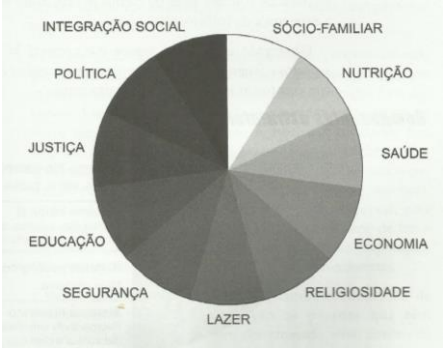

Figura 5: Universo social.
Fonte: (Ramos et al., 2008).

A complexidade do mundo interior individual está diretamente relacionada com aspectos individuais tais como percepção, afeição, realidade, sonhos, medos, desejos que são influenciados por aspectos do universo social tais como integração-social, sócio familiar, educação. Tais aspectos individuais refletem-se no coletivo, influenciam as relações e podem influenciar ou determinar medidas de controle de segurança mais ou menos rígidas.

2.8 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. É considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes, como, por exemplo, o conhecido "conto do vigário".
Conforme (MITNICK; WILLIAM, 2003), geralmente não é simples obter informações sigilosas de instituições de nichos de serviços críticos 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 enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.
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, o que aumenta a probabilidade de atração mútua. Podendo trazer vários benefícios como elevação da autoestima, sensação maior de felicidade e bem-estar, de ser entendido e estar seguro.
2. Farinha do Mesmo Saco: semelhanças conectam as pessoas. Encontrar coisas em comum rapidamente estabelece uma conexão e um ambiente fértil para desenvolver amizades. Aristóteles escreveu: "Nós gostamos daqueles que se parecem conosco e

que possuem os mesmos objetivos… Gostamos daqueles que desejam as mesmas coisas que nós".

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. Portanto, uma "isca de curiosidade" se torna uma ferramenta eficaz para conhecer alguém de interesse e desenvolver uma amizade.
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 na mesma medida ou num gesto ainda maior.
6. A Lei da Revelação Prévia: indivíduos que revelam mais informações pessoais possuem mais chances de receber em troca o mesmo nível de informação. Revelação prévia promove a atração. As pessoas sentem proximidade com outros que revelam suas vulnerabilidades, pensamentos íntimos e fatos sobre si mesmos.

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. Cialdini7, 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:

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

- Autoridade

As pessoas têm a tendência de atender a uma solicitação que é feita por uma pessoa com autoridade. Uma pessoa pode ser convencida a atender uma solicitação se ela acreditar que o solicitante é uma pessoa com autoridade ou que está autorizada a fazer tal solicitação.

- 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 aos da vítima.

- Reciprocidade

As pessoas podem atender automaticamente a uma solicitação quando recebem ou têm a promessa de receber algo de valor. O presente pode ser um item material, um conselho ou ajuda. Quando alguém faz algo para um indivíduo, o indivíduo sente uma inclinação em retribuir. Essa forte tendência de retribuir existe nas situações em que a pessoa que recebe o presente não pediu por ele.

- Consistência

As pessoas têm tendência de atender após fazer um comprometimento público ou adotar uma causa. Depois que prometem, fazem qualquer coisa, não querem parecer pouco confiáveis ou indesejáveis e tendem a seguir as instruções para serem coerentes com a declaração ou promessa.

- Validação social

As pessoas tendem a cooperar quando isso parece estar de acordo com aquilo que as outras pessoas estão fazendo. A ação dos outros é aceita como uma validação de que o comportamento em questão está correto e apropriado.

- 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, ou que ele só está disponível por um período de tempo curto.

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;
- Os códigos contábeis e ás cópias dos diretórios corporativos (uma cópia impressa, um arquivo de dados ou uma lista eletrônica de telefones na intranet) são alvos frequentes dos engenheiros sociais. Cada empresa precisa ter uma política escrita e bem divulgada sobre a revelação desse tipo de informação. As salvaguardas devem incluir a manutenção de um registro de auditoria que estabelece os casos em que as informações sigilosas para as pessoas de fora da empresa;
- 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. Seguir as políticas e os procedimentos da empresa com relação a verificação e a divulgação das informações não públicas;
- O treinamento de segurança com relação a política da empresa criado para proteger os ativos de informação precisa ser aplicado a todos que trabalham na empresa, e não apenas ao empregado que tem acesso eletrônico ou físico ao ativo de TI da 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 está autorizada: A pessoa tem a necessidade de saber ou tem autorização para fazer a solicitação?

2.9 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 ideias 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. É recomendado a criação e planejamento deste plano conforme a seguinte ordem e sequência de atividades:

- Definição do objetivo;
- Compreensão do universo que envolve o público alvo (atores desse cenário, seu status e papel, suas aspirações, padrões de comportamento, criatividade cultural[8]);
- Análise histórica da evolução da segurança na organização. E paralelamente estudo e compreensão do *business plan*[9]da empresa, sua missão e valores corporativos;
- Seleção e ordenamento, quanto a prioridade, dos conteúdos;
- Definição de metodologia de abordagem;
- Definição do intervalo de tempo entre a apresentação dos conteúdos.

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 [10]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.

2.10 Política de Segurança da Informação

Conforme Ramos et al, (2008) a política de segurança da informação de uma organização é um conjunto de documentos que descreve quais são os objetivos que todas as áreas ligadas a segurança da informação devem trabalhar para atingir.
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

[8] Caminho alternativo, a forma como as pessoas resolvem os seus problemas quando o caminho oficial não responde em tempo.
[9] Plano com diretrizes formais quanto aos objetivos de negócio, justificativas quanto a viabilidade de alcance dos objetivos e planos para alcança-los.
[10] 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.

comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização. Ela recomenda que a política contenha declarações relativas aos itens abaixo listados:

- Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação;
- Uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio;
- Uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco; breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:
    - Conformidade com a legislação e com requisitos regulamentares e contratuais;
    - Requisitos de conscientização, treinamento e educação em segurança da informação;
    - Gestão da continuidade do negócio;
    - Consequências das violações na política de segurança da informação.
- Definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;
- Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

3. 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 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.

Referência Bibliográfica

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. Acesso em: 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.

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

Sêmola, M. **Gestão da Segurança da Informação: Uma Visão Executiva**. Campus Elsevier: Rio de Janeiro, 2003. 154p.