Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

ENGENHARIA SOCIAL: UM ESTUDO DE CASO

EDLAINE DE OLIVEIRA AVELAR

Americana, SP
2018

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

ENGENHARIA SOCIAL: UM ESTUDO DE CASO

EDLAINE DE OLIVEIRA AVELAR
edlaine_avelar@hotmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec-Americana, sob a orientação da Profa. Dra. Acácia Ventura.

Área: Fator Humano e Engenharia Social

Americana, SP
2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

A967e AVELAR, Edlaine de Oliveira

Engenharia social: um estudo de caso. / Edlaine de Oliveira Avelar. – Americana, 2018.

47f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Dra. Acácia de Fátima Ventura

1 Segurança em sistemas de informação 2.Engenharia social I. VENTURA , Acácia de Fátima II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

EDLAINE DE OLIVEIRA AVELAR

ENGENHARIA SOCIAL: UM ESTUDO DE CASO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Fator Humano e Engenharia Social

Americana, 25 de junho de 2018.

Banca Examinadora:

Acácia Ventura (Presidente)
Doutora
FATEC – Americana

Marcus Vinícius Lahr Giraldi (Membro)
Especialista
FATEC – Americana

Márcio Roberto Baldo Taglietta (Membro)
Especialista
FATEC – Americana

AGRADECIMENTOS

Primeiramente agradeço a minha orientadora, Acácia Ventura, pelo auxílio durante o desenvolvimento do trabalho, pela paciência e por estar sempre disposta a ajudar e tirar duvida.

Ao meu namorado, Gustavo Gazzeta, pela paciência nos momentos mais complicados, por estar sempre presente e ser compreensivo nos momentos estressantes.

A Minha família por sempre me motivar a continuar o curso, apesar de todas as dificuldades e por todo o apoio que me concederam nesses anos todos.

Aos alunos do Curso de Tecnologia em Segurança da Informação que prontamente responderam as questões, para que o estudo de caso pudesse ter sido feito, o meu muito obrigado.

Agradeço também aos que de alguma forma se envolveram nesse projeto, toda a colaboração foi muito bem recebida e muito importante para que ele fosse desenvolvido.

DEDICATÓRIA

Aos meus pais e meu namorado, por me apoiarem em todos os momentos de dificuldades enfrentados.

À Deus, por me dar forças para continuar, sempre seguindo em frente e buscando pelo melhor.

EPIGRAFE

“Somente duas coisas são infinitas: o Universo e a estupidez humana. E não estou seguro quanto à primeira”. (Albert Einstein)

RESUMO

A segurança da informação tem se tornado, cada vez mais, indispensável para todas as companhias. Empresas que trabalham com Tecnologia da informação precisam de um cuidado maior para evitar o vazamento de dados sigilosos, pois com a tecnologia existente nessas organizações a chance de ocorrer acessos não autorizados é maior. Grande parte dessas empresas investe em *firewalls* e antivírus para se protegerem de *hackers*, trabalhando em evitar uma entrada pela rede, mas não tem uma política de segurança eficaz e nem treinamentos adequados para seus funcionários, com isso criam-se aberturas para ataques de engenharia social. Assim, este trabalho, através de pesquisa qualitativa e quantitativa, tem como objetivo realizar um estudo de caso entre os alunos de segurança da informação da FATEC Americana, por meio de um questionário desenvolvido pelo autor e aplicado para alunos, que trabalham ou trabalharam em empresas de T.I.,nos seis semestres do período noturno, com intuito de perceber o desenvolvimento de seus conhecimentos no decorrer do curso em relação a engenharia social,analisar se eles cumprem a política de segurança para evitar possíveis ataques de engenharia social e como seria a reação desses alunos caso presenciassem uma tentativa de acesso, físico ou por telefone, de um engenheiro social. Após a análise dos questionários respondidos, pôde-se observar que, mesmo com conhecimento sobre engenharia social e a importância de políticas de segurança, muitos dos alunos questionados, assumiram não cumprir as regras da empresa, na maioria dos casos, por seus superiores não demonstrarem a importância dessas normas, além de algumas empresas não terem uma política de segurança. Com isso pode-se perceber que, mesmo com profissionais especializados em segurança da informação, as empresas ainda não compreendem ou não aceitam os riscos da engenharia social.

Palavras chaves: Segurança da informação; engenharia social; política de segurança.

ABSTRACT

The information security is becoming, more and more, indispensable for all companies. Enterprises which work with Information Technology need greater care to avoid the exposure of sensitive data, because with the existing technology within those companies, the chance of not authorized access occurring is higher. Most of these companies invest in firewalls and anti-virus to protect from hackers, working to avoid an opening through the network, but there is neither an effective security policy nor an appropriate training to the employees, thereby creating openings for social engineering attacks. Thus, this work, through qualitative and quantitative research, aims to perform a case study among the information security students of FATEC Americana, by means of a questionnaire developed by the author and applied to the students, who either work or worked on I.T companies, in the six semesters of the night period, in order to perceive their knowledge development during the course regarding social engineering, analyze if they comply the security policy to avoid possible social engineering attacks and how would be the reaction of these students if they witnessed an access attempt, physical or by phone of a social engineer. After the analysis of the answered questionnaires, it could be observed that, even with the knowledge around social engineering and the importance of the security policies, many of the questioned students, assumed not to comply with the company rules, in most cases, by their superiors not demonstrating the significance of these standards, besides some of the companies not having a security policy. Thereby, it can be seen that, even with specialized professionals in information security, the companies still do not comprehend or accept the risks of the social engineering.

Keywords: Information security; social engineering; security policy.

LISTA DE FIGURAS E DE GRÁFICOS

Figura 1 - Fatores principais na segurança de informática.....21

Figura 2 - Vetores de análise de integração de segurança empresarial em informática.....22

Figura 3 - Ciclo da administração de segurança empresarial.....30

Figura 4 - Fluxo de análise de ameaças e riscos.....31

Figura 5 - Sequência das etapas de implantação da segurança.....32

Figura 6 - Controle em operações e saídas de informações.....33

Gráfico 1 - Conhecimento sobre engenharia social.....36

Gráfico 2 - A empresa na qual trabalha tem abertura para um ataque de engenharia social.....36

Gráfico 3 - História que conhecem de tentativa de entrada não autorizada na empresa.....37

Gráfico 4 - Existência de política de segurança onde trabalha.....37

Gráfico 5 - Cumprimento da política de segurança onde trabalha.....38

Gráfico 6 - Cumprimento da política de segurança pelos superiores.....39

Gráfico 7 - dificuldade para conseguir informações sigilosas na empresa, sem a devida autorização.....39

Gráfico 8 - Passaria uma informação de caráter sigilosa para uma pessoa que ele não tem certeza que tem a devida autorização.....40

SUMÁRIO

INTRODUÇÃO 9

1 SEGURANÇA DA INFORMAÇÃO E ENGENHARIA SOCIAL 14

1.1 SEGURANÇA DA INFORMAÇÃO 14

1.1.1 Pilares da segurança da informação. 19

1.2 ENGENHARIA SOCIAL 23

1.2.1 Se defendendo de um engenheiro social 29

2 ESTUDO DE CASO 35

2.1 IDENTIFICAÇÃO DA POPULAÇÃO E INSTRUMENTO UTILIZADO 35

3 CONSIDERAÇÕES FINAIS 42

4 REFERÊNCIAS 44

APÊNDICE 01 48

INTRODUÇÃO

Atualmente um dos campos mais importantes da área de segurança é a de segurança da informação, uma vez que, quase todas as empresas possuem um sistema informatizado. Em muitas empresas não se da à devida seriedade a essa área e isso gera portas que podem ser utilizadas para um acesso não autorizado às informações da corporação. Em alguns casos o próprio site comercial da empresa pode fornecer informações de mais, o que possibilita e facilita um acesso não autorizado aos dados da empresa. Nomes de funcionários, acontecimentos recentes da empresa, localizações de filiais, entre outros informes, podem ser utilizados por invasores para convencer empregados inexperientes ou mal informados de que tem envolvimento com a empresa.

> Se você é uma daquelas pessoas que pensa 'oh, essa coisa de busca no Google não é muito útil num teste de segurança (...) isso é só jogada', você não tem ideia do que esta falando. Quando conduzimos um teste detalhado de segurança, é preciso separar pelo menos um ou dois dias para uma investigação completa, a fim de conhecer um pouco nosso alvo antes de usar um único pacote com um scanner. Se conseguirmos que o cliente nos de mais tempo, realizamos uma investigação ainda mais a fundo, começando com um interrogatório completo de nossa ferramenta favorita de reconhecimento, o Google. (LONG, 2005, s/ p.)

Com falhas na segurança da informação, podem ser abertas várias portas para pessoas mal-intencionadas que desejam obter algo de uma determinada companhia, mas nem sempre essa invasão é feita somente pela rede ou internet. Uma abertura muito utilizada e, às vezes, até mais eficiente é a engenharia social, que consiste em usar a persuasão e mentiras para enganar alguém e conseguir tirar vantagem e informações dessa pessoa.

> 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 e SIMON, 2003, p.03)

O fator humano é descrito por muitos autores como o elo mais fraco da segurança, pois, segundo eles, não adianta ter a mais atual tecnologia quando os envolvidos não entendem a importância de proteger os dados confidenciais da organização. Algumas empresas não possuem uma política de segurança para acessos a informações restritas e, com isso, esses dados acabam ficando desprotegidos de pessoas com intenções maliciosas. Além de ser a maior abertura para a engenharia social, que para Rufino (2002, p.26) é: “uma técnica que não requer prática nem tão pouco habilidade, basta ter poder de convencimento e uma pitada de psicologia comportamental. Quando é bem executada é de uma eficiência surpreendente e normalmente não deixa rastros”.

Segundo Mitnick e Simon (2003, p.05) “o problema não é se isso acontecerá, mas sim quando acontecerá”.

Esse trabalho tem a finalidade de analisar os riscos de segurança que a engenharia social pode oferecer para empresas de todos os portes.

O estudo se **justificou** pela importância de existir uma segurança apropriada e “garantida” para os dados importantes e confidenciais, para garantir que os mesmos não sejam acessados por pessoas não autorizadas ou mesmo invasores, com o intuito de conseguir essas informações para uso próprio ou para vendê-las.

O **problema** encontrado para o desenvolvimento desse estudo foi observar que muitas empresas não têm uma política de segurança para evitar a entrada de pessoas estranhas, ou o acesso aos dados sigilosos por pessoas não autorizadas. Além de essas organizações não se prevenirem contra o ataque de engenheiros sociais com foco no fator humano, por não acreditarem que a empresa tenha abertura para esse tipo de ataque.

As **hipóteses** foram: a) A realização de o trabalho ocorrer sem dificuldades, encontrando os materiais necessários para pesquisa e pessoas que trabalhassem na área de tecnologia da informação que tivessem tido experiências negativas com engenharia social; b) Existir certa dificuldade para encontrar o material imprescindível e indispensável para a realização das observações e exploração da

área, e ainda houver contratempos para encontrar indivíduos para realizar a coleta de dados através do questionário; e, c) Algum obstáculo impedir que o trabalho seja entregue a tempo e que a pesquisa e o estudo de caso não possam ser realizados, seja por falta de recursos ou por outros motivos que bloqueiem a concretização do projeto em questão.

O **objetivo geral** foi: estudar e entender a engenharia social e seus riscos para as companhias, objetivando identifica-los em empresas de TI, através de pesquisa com docentes e alunos que trabalham na área.

Os **objetivos específicos** foram: A) Fazer uma pesquisa sobre o que é a engenharia social e seus riscos, para entender seus efeitos; B) Criar um estudo de caso composto de questionários para docentes e alunos da FATEC que trabalhem ou tenham trabalhado em empresas de grande, médio e pequeno porte de T.I, para obter dados de casos que aconteceram nessas empresas e analisar falhas que as companhias muitas vezes desconhecem; e, C) Analisar os dados obtidos com a pesquisa de campo, para estudar as implicações que a engenharia social pode causar em corporações e explorar as possibilidades de melhoras para evitar esse tipo de ataque.

O **Método** utilizado foi o hipotético-dedutivo, que para Popper (apud MARCONI e LAKATOS, 2009, p. 95) é: “A observação não é feita no vácuo. Tem papel decisivo na ciência. Mas toda observação é precedida por um problema, uma hipótese, enfim algo teórico. A observação é ativa e seletiva, tendo como critério de seleção as “expectativas inatas”. Só pode ser feita a partir de alguma coisa anterior. Esta coisa anterior é nosso conhecimento prévio ou nossas expectativas. Qualquer observação escreve Popper (1977, p.58):

> É uma atividade com um objetivo (encontrar ou verificar alguma regularidade que foi pelo menos vagamente vislumbrada); trata-se de uma atividade norteada pelos problemas e pelo contexto de expectativas (‘horizonte de expectativas’). Não há experiência passiva. Não existe outra forma de percepção que não seja no contexto de interesse e expectativas, e, portanto, de regularidades e leis. Essas reflexões levam-me a suposição de que a conjectura ou hipótese precede a observação ou percepção; temos expectativas inatas, na forma de expectativa latentes, que há de ser ativadas por

> estímulos aos quais reagimos, via de regras, enquanto nos empenhamos na exploração ativa. Todo aprendizado é uma modificação de algum conhecimento anterior.

A **pesquisa** foi classificada de acordo com sua natureza como básica, que para Chehuen Neto (2012, p.102): “Objetiva a produção de novos conhecimentos, úteis para o avanço da ciência, sem uma aplicação prática prevista inicialmente. Pode ser vista como ‘o saber pelo saber’. Envolve verdades e interesses universais. É útil para se avaliar a teoria, compreender, explicar e predizer relações entre fenômenos. Pode ter cunho eminentemente intelectual”.

Para a abordagem do problema foram utilizadas as pesquisas qualitativa e quantitativa, que para Chehuen Neto (2012, p. 102-103) são: Pesquisa Quantitativa:

> Eventualmente chamada de pesquisa fechada, pressupõe que tudo pode ser quantificável, como por exemplo, os estudos das ciências biológicas, até opiniões ou outras informações (ciências humanas e sociais), como atitudes e comportamentos e assim, classificá-las e analisá-las. Utiliza diferentes técnicas estatísticas para validar a pesquisa. Utiliza o procedimento experimental, faz interferência a partir das amostras, testa hipóteses e teorias.

E a Pesquisa Qualitativa:

> Considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa. Não requer uso de técnicas estatísticas. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento-chave.

Para que os objetivos fossem atingidos utilizou-se a pesquisa descritiva, que para Rampazzo (1998, p.58) é aquela que: “[...] observa, registra, analisa e correlaciona fatos ou fenômenos (variáveis), sem manipulá-los; estuda fatos e fenômenos do mundo físico e, especialmente, do mundo humano, sem a interferência do pesquisador”.

Para os procedimentos técnicos foram utilizadas as pesquisas bibliográfica, levantamento e estudo de caso. A pesquisa bibliográfica, de acordo com Marconi e Lakatos: (2012, p.185) pode também ser chamada de fontes secundárias

> [...] abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico etc., até meios de comunicação orais: rádio, gravações em fita magnética e audiovisuais: filmes e televisão. Sua finalidade é colocar o pesquisador em contato direto com tudo que foi escrito, dito ou filmado sobre determinado assunto, inclusive conferências seguidas de debates que tenham sido transcritas por alguma forma, quer publicadas, quer gravadas.

E o estudo de caso é descrito por Sampieri, Collado e Lucio (2006, p. 274) como: “[...] não é uma escolha do método, mas do “objeto” ou da nossa “amostra” que serão estudados”. E ainda complementam: “O estudo de caso é tanto de corte quantitativo (...) como de corte qualitativo (...) ou inclusive misto”.

O estudo foi desenvolvido em três capítulos, no primeiro são apresentados os conceitos de segurança da informação e engenharia social, analisando os riscos existentes para as empresas de Tecnologia da Informação (T.I.), os principais métodos utilizados pelos engenheiros sociais e as melhores formas de evitá-los. No segundo capítulo o leitor encontrará a análise de um estudo de caso feito com alunos do Curso Superior de Tecnologia em Segurança da informação da FATEC Americana, que responderam a um questionário sobre engenharia social e seus riscos para as empresas. O terceiro capítulo foi reservado as considerações finais.

1 SEGURANÇA DA INFORMAÇÃO E ENGENHARIA SOCIAL

O capítulo conceitua informação, ressalta a seu papel nas empresas e, principalmente, a importância de sua segurança, e, apresenta a engenharia social, seus principais riscos e maneiras de evitá-la.

1.1 SEGURANÇA DA INFORMAÇÃO

Para falar de segurança da informação considera-se importante recordar nas palavras de Oliveira (2005, p.34) que: “Entramos, há poucas décadas na era da informática, e uma nova ruptura se estabelece. Da estabilidade de linguagem representada estatisticamente nos livros, passa-se à instabilidade da linguagem eletrônica. Dos escribas aos internautas”. E ainda “A informação se apresenta digitalizada e virtualizada, não mais restrita ao suporte do papel. Do texto impresso (...) ao processado; do livro impresso ao l(...) eletrônico”.

E Caruso e Steffen (2006, p.23) destacam que ao longo da história:

> [...] o ser humano sempre buscou o controle sobre as informações que lhe eram importantes de alguma forma; isso é verdadeiro mesmo na mais remota antiguidade. O que mudou desde então foram as formas de registro e armazenamento das informações; se na Pré-história e até mesmo nos primeiros milênios da idade antiga o principal meio de armazenamento de informações era a memória humana, com o advento dos primeiros alfabetos isso começou a mudar. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas.

Atualmente a Segurança da informação é tratada como fator primordial para qualquer empresa que entenda a importância da proteção de seus dados. Para o site Conceito.de (2011, s/p) o significado de segurança: “[...] Refere-se à qualidade daquilo que é seguro, ou seja, àquilo que está ao abrigo de quaisquer perigos, danos ou riscos... ”. A palavra deriva do latim securĭtas.

Já informação para Fontes (2006, p.2): “[...] É um recurso que move o mundo, além de nos dar conhecimento de como o universo esta caminhando”. E complementa: “Informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor profissional”.

Para facilitar o entendimento do conceito de informação Wurman (1991, apud OLIVEIRA, 2004, p. 30-31), divide a informação em cinco anéis:

> - O primeiro anel é o da informação interna. São as mensagens que governam o nosso sistema interno e possibilitam o funcionamento do nosso corpo. Aqui a informação toma forma de mensagens cerebrais. Provavelmente, temos um controle menor sobre esse nível de informação do que sobre os outros, mas é o que mais nos afeta.
>
> - O segundo anel é o da informação Conversacional. São as trocas formais e informais, as conversas que mantemos com as pessoas a nossa volta, sejam amigos, parentes, colegas de trabalho, estranhos na fila de embarque ou clientes e, reuniões de negócios. A conversa – talvez por sua natureza informal – constitui uma importante fonte de informação, embora nossa tendência seja desprezar ou ignorar seu papel. E, no entanto, esta é a fonte de informação que mais exercemos controle, tanto como emissores quanto como receptores de informação.
>
> - O terceiro anel é o da informação de referência. Aqui nós voltamos para a informação que opera os sistemas do nosso mundo – ciência e tecnologia – e, mais imediatamente, para os materiais de referências que usamos em nossa vida. A informação de referência pode ser qualquer coisa desde um manual de física quântica ate a lista telefônica ou o dicionário.
>
> - O quarto anel é o da informação noticiosa. Ela abrange os eventos da atualidade – a informação transmitida pela mídia sobre as pessoas, lugares e acontecimentos, que talvez não afetem diretamente a nossa vida, mas podem influenciar nossa visão de mundo.
>
> - O quinto anel é o da informação cultural. Está é a menor forma quantificável. Abrange história, filosofia e a arte, qualquer expressão de uma tentativa de compreender e acompanhar nossa civilização. Informações colhidas nos outros anéis são incorporadas aqui para construir o conjunto que determina nossas atitudes e crenças, bem como a natureza de nossa sociedade como um todo.

Menezes (2006, p.26-27) acredita que: “No século XXI, a velocidade com que as informações e o conhecimento fluem estabelecem a necessidade de estratégias suportadas por novos referenciais e o desenvolvimento de modelagens mentais alinhadas com os riscos desse novo ambiente de negócios”.

Após entender o que de fato é informação e sua importância em uma empresa, existe a necessidade de compreender que é fundamental garantir sua segurança. Fontes (2006, p.2) classifica a segurança da informação como: “[...] O

conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada".

Caruso e Steffen (2006, p.23) fazem uma analogia da segurança da informação com um ditado popular: "nenhuma corrente é mais forte que seu elo mais fraco":

> [...] da mesma forma, nenhuma parede é mais forte que sua porta ou janela mais fraca, de modo que você precisa colocar as trancas o mais resistente possível nas portas e janelas. De forma similar, quando você implementa segurança em um ambiente de informações, o que na realidade você esta procurando fazer é eliminar o máximo possível de pontos fracos ou garantir o máximo de segurança possível para eles.

Ferreira e Araújo (2008, p.07) acreditam que a segurança da informação é: "[...] relativamente nova em comparação com as outras áreas do conhecimento humano, embora os sistemas de controle de confidencialidade, tais como a cifragem, a criptografia ou a guarda de documentos em cofres, existam desde os primórdios da história".

Mesmo nova tornou-se fundamental para as pessoas e para as organizações, em maior ou menor grau. "E o grau de dependência agravou-se (...) em função da tecnologia de informática, que permitiu acumular grandes quantidades de informações em espaços restritos. O meio de registro é, ao mesmo tempo, meio de armazenamento, (...) de acesso e (...) de divulgação". (CARUSO e STEFFEN 2006, p.24)

Gil (1998, p.13), ressalta que a: "Segurança é responsabilidade de todos, ou seja, dos profissionais de informática e das áreas usuárias (...) incorporada ao desempenho de suas funções, as tarefas de criação, atendimento e monitoração da visão de segurança".

> Sabendo que a informação armazenada nos computadores da empresa ou em outros meios possui um alto valor para a continuidade dos negócios, o profissional de segurança deve se preocupar com o todo. A visão empresarial deve ser um pré-requisito

> de qualquer profissional, isso inclui o de segurança da informação. Entretanto, a generalização da proteção, sem considerar os fatos críticos de sucesso, sem identificar os processos importantes para o dia-a-dia da empresa e outras questões-chave, pode estar consumindo fortunas, sem retorno efetivo para a empresa e/ou sem estar protegendo o que realmente precisa ser protegido. (DAWEL, 2005, p. 18).

Manter os computadores com *firewalls* e antivírus sempre atualizados e compatíveis com a utilização de cada máquina torna-se imprescindível para evitar invasões pela rede, mas estes não são tão eficazes quando não existem precauções de seguranças nas atividades dos usuários.

> O *firewall* pode ser comparado aos muros que foram construídos ao redor da propriedade. Este muro virtual possui algumas aberturas (ou portas) pelas quais a informação flui nos dois sentidos (informação entra, informação sai). Este recurso possui um mecanismo de filtros que determina o que pode entrar e o que pode sair, (sic) baseado em regras configuradas pelos administradores e obedecendo a definições estabelecidas nas políticas da companhia. São semelhantes aos guardas na portaria e recepção: ambos fiscalizam e liberam ou não o acesso ao interior da empresa. Note que, da mesma maneira que alguém pode se fazer passar por um funcionário e enganar os guardas da portaria, o "firewall" pode ser enganado e deixar passar coisas que não poderiam entrar. (DAWEL, 2005, p. 45).

Menezes (2006, p.41), afirma: "Um *firewall* não impede o vazamento de dados. (...) não existe apólice de seguro contra estupidez, se um funcionário fornece sua senha de acesso a usuários não autorizados ou desconhecidos, não há *firewall* que resolva".

Para Gil (1998, p.103) a segurança deve está nas entranhas da cultura organizacional: "[...] Desta forma, normas existentes, procedimentos e práticas administrativas/técnicas/operacionais, cumpridas pelos profissionais das organizações, são determinantes do nível da segurança empresarial em informática".

Existem diversos fatores que podem prejudicar a segurança da informação. Para Dawel (2005, p. 48): "Todos os elementos que estão do lado de fora (quer sejam equipamentos, programas ou pessoas, incluindo-se aí os funcionários, prestadores de serviço, executivos e acionistas. São ameaças potenciais contra a

segurança da informação". E acrescenta: "Em outras palavras, proteger a informação transcende os limites da tecnologia".

> [...] A segurança é um assunto que envolve todos dentro da empresa, exige cooperação e é um processo demorado. Ela terá um impacto considerável no ambiente informacional na empresa. Além disso, é uma tarefa de longo prazo e pode exigir grande dispêndio de recursos, ainda que a cada dia seja mais necessária, devendo, portanto, ser cuidadosamente planejada e executada para que não venha a se converter em mais um problema. (CARUSO e STEFFEN 2006, p.36)

Um dos maiores inimigos da segurança da informação são os hackers que, segundo o dicionário online de língua portuguesa Dicio (2009, s/p), é: "Quem invade sistemas computacionais ou computadores para acessar informações confidenciais ou não autorizadas, apontando possíveis falhas nesses sistemas".

Em muitos casos as empresas tendem em trabalhar na proteção da rede, para evita o ataque desses hackers, pois se acredita que são pessoas desconhecidas e que não tem acesso físico à empresa. Além de muitas empresas acreditarem que não tem abertura para uma invasão física.

> Talvez você concorde plenamente que os "hackers" e "crackers" estão do lado de fora. Neste ponto parece fácil separar e afirmar com mais certeza, pois eles não fazem parte da relação funcional e nem comercial. Será? Afinal, quem são esses seres sem nome? Será que esses "desconhecidos", que se escondem atrás de apelidos, possuem documentos de identidade? Passaporte? Eles nasceram e vivem em algum lugar desse planeta? Será que fizeram curso superior e trabalham para alguma empresa? Quem sabe na sua empresa? Talvez no mesmo andar, na sala ao lado ou na mesa a sua frente? Quem sabe é o faxineiro? Ah, essa não! Quem liga para o faxineiro? O pessoal da faxina circula livremente pela sua empresa e ninguém se da conta de quem são. Quem garante que o faxineiro não é especialista em ciência da computação? Ou foi infiltrado para coletar informações que estão espalhadas pela empresa de diversas formas? (DAWEL 2005, p. 26).

Por isso a atenção deve ser redobrada para que não sejam passados dados confidencias para pessoas não autorizadas, mesmo que estas trabalhem na mesma empresa. Gerentes, executivos e outras pessoas com cargos superiores devem ter mais cuidado, pois tem acesso a informações de suma importância para a empresa

e precisam estar atentos com o ambiente e, principalmente, com as pessoas quando falam de alguma informação da empresa.

Fontes (2006, p. 121) destaca cuidados necessários quando se trata de informações da organização, são elas:

> Falar em ambientes não seguros – A vontade de resolver problemas nos leva a continuar reuniões no elevador, no taxi e em outros locais sem privacidade. [...]
>
> Mostrar a informação – Gosto muito de viajar na poltrona do corredor do avião. Aprendo muito vendo as diversas apresentações que os executivos revisam no seu computador. Os minutos da ponte aérea são valiosos, e, o executivo aproveita para abrir seu notebook e acaba mostrando para os vizinhos algumas informações da organização.
>
> Deixar informação – Ao sair do local de reunião, os quadros, as folhas de *flip charts*, os papéis de rascunho e outros materiais devem ser retirados, apagados ou destruídos. [...]
>
> Entregar a informação – Muitas informações são colocadas no lixo sem serem devidamente destruídas. [...]
>
> Acesso físico – As áreas e os ambientes físicos da organização devem ter acesso restrito para visitantes e outras pessoas que não trabalham no local no dia-a-dia.

Tendo em vista a importância da segurança da informação para o ambiente empresarial, é importante destacar os principais fundamentos para garantir que as informações estejam seguras e sejam confiáveis.

1.1.1 Pilares da segurança da informação.

Para que exista segurança da informação é necessário uma série de fatores. Oliveira (2004, p.23) descreve que: “Em muitos aspectos a informação é ideal para transmitir o conhecimento explícito; é rápida, segura e independente de sua origem. Essas três características são de vital importância na era da tecnologia porque o computador foi criado para lidar com informações”.

Existem três “pilares” que são considerados primordiais no quesito de segurança da informação: Confidencialidade, disponibilidade e integridades, embora muitos autores já defendam que existem outros pontos extremamente importantes quando o assunto é informação, como: Autenticidade, não repúdio, legalidade, privacidade e auditoria.

> • Confidencialidade. A informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso.
>
> • Disponibilidade. A informação deve estar disponível no momento em que a mesma for necessária.
>
> • Integridade. A informação deve ser recuperada em sua forma original (no momento em que foi armazenada). É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.
>
> • Autenticidade. Garante que a informação ou o usuário da mesma é autêntico.
>
> • Não repúdio. Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; não é possível negar o envio ou recepção de uma informação ou dado.
>
> • Legalidade. Garante a legalidade (jurídica) da informação; a aderência de um sistema à legislação; e as características das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação nacional ou internacional vigente.
>
> • Privacidade. Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve poder ser vista / lida / alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste caso é atribuído o caráter de confidencialidade à informação). É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.
>
> • Auditoria. Rastreabilidade dos diversos passos de um negócio ou processo, identificando os participantes, os locais e horários de cada etapa. A auditoria aumenta (LAUREANO; MORAES, 2005 p.41).

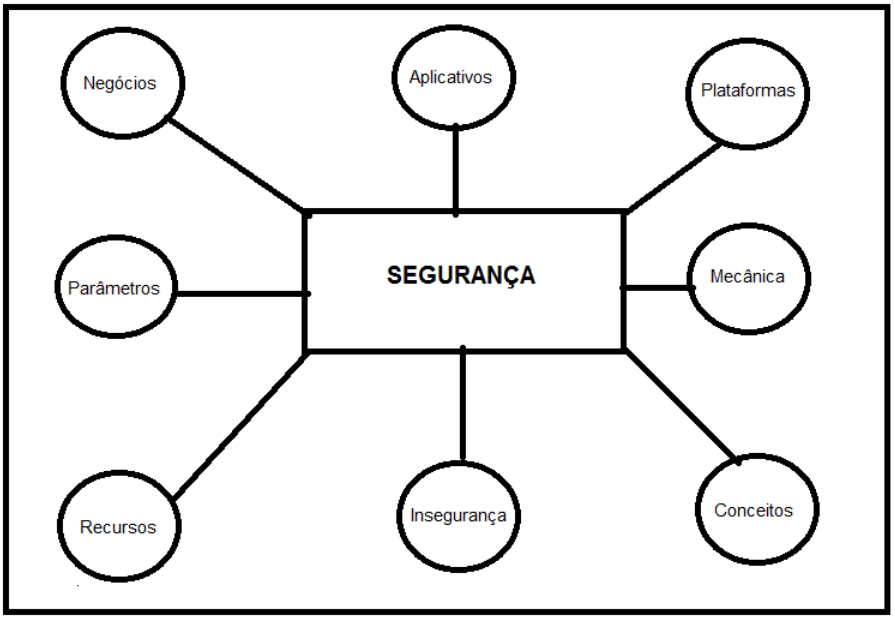
Esses chamados “pilares” formam a base fundamental para que a informação seja confiável e sempre segura de vulnerabilidades, que para Lyra (2008, p06), são: “Fraquezas que podem gerar, intencionalmente ou não, a indisponibilidade, a quebra de confidencialidade ou integridade. A vulnerabilidade de um ativo é seu ponto fraco”. Além de também se manter a salvo de ameaças que segundo Lyra (2008, p. 6): “É um ataque em potencial a um ativo da informação. É um agente externo que, aproveitando-se da vulnerabilidade, poderá quebrar um ou mais dos três princípios de segurança da informação”.

Existem também muitos fatores que podem interferir na segurança da informação, como se pode observar nas figuras 1 e 2.

Figura 1: Fatores principais na segurança de informática.

Fonte: CARUSO e STEFEN (2006, p.42).

Figura 2: Vetores de análise de integração de segurança empresarial em informática.



Fonte: GIL (1998, p.37).

Para proteger os dados confidenciais de uma corporação existem vários tipos de softwares, antivírus, firewalls, programas, sites e até mesmo cargos na empresa que tem foco em guardar as informações, mas em muitos casos isso não é o suficiente, pois as pessoas envolvidas podem acabar por entregar informações confidenciais por inexperiência ou ingenuidade. Muitas vezes, existe a falsa sensação de segurança por ter um equipamento seguro, mas existem muitas vulnerabilidades, pois os funcionários não compreendem a importância de manterem seus conhecimentos para si próprios.

> Cada pessoa que trabalha para a empresa precisa ter em mente esse objetivo, tornando-se, assim, um colaborador para os objetivos da empresa e para seus objetivos pessoais. Esta é a primeira convergência necessária. Melhor seria se cada pessoa se tornasse um acionista; desta forma, a pessoa estaria na condição de ser seu próprio colaborador, sentindo no bolso o resultado de seu esforço pessoal, associado ao desempenho dos demais colegas. (DAWEl, 2005, p. 102)

Por muitas vezes os funcionários não compreenderem, ou não se importarem, com a gravidade e os riscos que suas ações irregulares podem gerar para a empresa, eles acabam criando brechas para invasores. É nesse ponto onde o engenheiro social vai atacar.

1.2 ENGENHARIA SOCIAL

A engenharia social, em muitos casos, recebe uma importância menor do que necessitaria. As empresas costumam acreditar que caso haja um ataque às informações, este será naturalmente através dos computadores. Para Peixoto (2006, p.04), a 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” e ainda relata “Não se trata de hipnose ou controle da mente, as técnicas de engenharia social são amplamente utilizadas por detetives (para obter informações) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos”.

> Quando você acessa um ambiente computacional, é necessário fazer a identificação e a autenticação. Cada vez mais esses procedimentos estão se sofisticando.
>
> A comunicação entre os computadores também esta ficando cada vez mais protegida. Utiliza-se a criptografia, técnica que possibilita que os textos se tornem ilegíveis, pois eles se transformam em uma cadeia de caracteres que não entendemos. Essa transformação é feita com sofisticados algoritmos matemáticos que exigem muitos recursos de computadores e de tempo para que sejam decifrados. Isso torna a opção de quebra de algoritmo descartáveis para a maioria das ações de má-fé.
>
> Sendo assim quando alguém deseja invadir ou acessar informações de uma organização, é muito mais fácil ir pelo caminho da engenharia social. (FONTES 2006, p. 120)

Em muitos casos o engenheiro social não precisa de um disfarce, nem mesmo de criar explicações para o motivo dele estar fazendo determinada pergunta. Peixoto (2006, p.8) diz: “Quando você tem alguma duvida ou que saber alguma informação, o que você faz é naturalmente pedir. Então nada mais prático do que simplesmente solicitar o pedido da informação interessada para a suposta vitima”. Por este motivo é de extrema importância uma política de segurança da informação rígida e um treinamento intenso para os funcionários que tem acesso a informações que não podem ser passadas para qualquer pessoa.

Mesmo com todo o conhecimento atual ainda existem pessoas simples e com pouca informação, ou pouco treinamento, para saber reagir a um ataque de um engenheiro social e acabam confiando em um desconhecido, liberando o acesso a informações importantes pessoais ou da empresa em que trabalha.

> O número de golpes aplicados por estelionatários usando os meios eletrônicos tem aumentado. São cada vez mais frequentes em São Paulo, por exemplo, os casos de falsa devolução de contribuição provisória sobre movimento financeiro (CMPF). Os criminosos telefonam para pessoas dizendo que são funcionários de bancos e comunicam e comunicam que o governo autorizou a devolução de 30% a 40% do imposto cobrado nos últimos anos. (FONTES, 2006 p.116)

Existem também casos em que o engenheiro social oferece ajuda para alguém que possua informações que ele deseje com o intuito de ter acesso a essas informações. Para Peixoto (2006, p 10) essa é conhecida como a técnica “posso ajudar?” Que ele descreve como: “O atacante, com sua habilidade nata de persuasão, consegue criar um problema para você. E aproveitando esse eventual problema criado, o engenheiro social passa a ser definitivamente a solução exata para os seus problemas”.

As empresas devem sim se proteger contra hackers, mas é fundamental reconhecer a existência do engenheiro social, o mal que ele pode causar e também a diferença do modo de agir entre um hacker e um engenheiro social.

> O hacker é um primo longe do engenheiro social. Nem todo engenheiro social é um hacker, mas em alguns casos o hacker chega a ser um engenheiro social, com condutas semelhantes a captura de informações. O hacker age de forma a explorar muito mais as vulnerabilidades técnicas, enquanto o engenheiro social explora as vulnerabilidades humanas. (PEIXOTO, 2006 p.17)

Outro ponto importante a ser considerado é o fato de o engenheiro social estar infiltrado dentro da empresa ou ter contato com alguém que trabalha ou trabalhou naquela organização, fazendo um controle de acesso rigoroso e sempre procurando conhecer ao máximo as pessoas que estão acessando informações valiosas e, acima de tudo, sigilosas.

> Quando um engenheiro social sabe como as coisas funcionam dentro da empresa-alvo, ele pode usar esse conhecimento para desenvolver a confiança junto aos empregados. As empresas precisam estar preparadas para os ataques da engenharia social vindo de empregados ou ex-empregados, que podem ter um motivo de descontentamento. As verificações de histórico podem ser uteis para detectar os candidatos a emprego que tenham uma propensão para esse tipo de comportamento. Mas na maioria dos casos é difícil detectar essas pessoas. A única segurança razoável nesses casos é implantar e auditar os procedimentos de verificação de identidade, incluindo o status de emprego da pessoa, antes de divulgar qualquer informação para qualquer um que não conheça pessoalmente e, portanto, não se sabe se ainda esta na empresa. (PEIXOTO, 2006 p.20).

Muitas pessoas ainda não perceberam que a falta de segurança da informação pode ter efeito na vida delas e não somente na empresa onde elas trabalham, esse é um dos motivos pelo qual ainda existem divulgações indevidas de dados importantes. Reinhold Spandl, gerente de soluções da empresa módulo *security solutions*, em uma entrevista ao site *cryptoid*, ressalta a importância de todas as pessoas entenderem as consequências de vazamentos de informação.

> Pode parecer que não, mas ainda hoje a maioria das pessoas, em sua vida particular (sic), não possuem a real percepção dos riscos a que estão expostas em função do mundo digital e da velha e perigosa engenharia social. A conectividade atual aliada a engenharia social acarretou uma elevação exponencial dos riscos, como por exemplo (sic) os sites de relacionamento que se apresentam como um ambiente com considerável número de crimes acontecendo. Então a primeira coisa a ser feita é desmistificar que a gestão de riscos é algo que diz respeito somente às empresas e instituições do Estado, a mesma é o processo base da segurança da informação, mas também está presente em nossas vidas! (SPANDL, 2016 s/p).

Fontes (2006, p. 122) recomenda: “Se alguém precisar falar com uma pessoa da organização, não passe os dados pessoais dela. Prefira sempre repassar os dados da pessoa de fora para a da organização e, se for o caso, será estabelecido o contato”.

Spandl (2016, s/p.) acrescenta que: “É fato que pessoas são o elo mais fraco na segurança da informação, mas não estamos fazendo a abordagem incorreta na hora de sensibilizá-los?”, pois é evidente que muitas empresa não entendem que funcionários conscientes são mais eficientes que os softwares de segurança para impedir invasão, se um colaborador não tem noção da importância da política de

privacidade da empresa, o mesmo não a levará a sério, assim a entrada de pessoas não autorizadas e invasores se torna muito mais fácil, pois um atacante nem sempre necessita de códigos para invadir um sistema. Muitas vezes ele pode apenas usar da engenharia social para conseguir informações valiosas, simplesmente se passando por um gerente ou alguém envolvido com a empresa.

> A engenharia social, de uma forma bem simplista, tem por objetivo de manipular pessoas e/ou acessar informações para fins dos mais diversos, desde um sequestro até mesmo uma simples abordagem para relacionamento pessoal. É pura manipulação das fraquezas e ingenuidades que todos nós temos, e não há como impedir! Quem já não caiu em uma brincadeira de um amigo porque iria se dar bem? Mas pode-se reduzir a probabilidade de sucesso de uma abordagem por engenharia social, capacitando e treinando as pessoas para que, por exemplo:
>
> Desconfie da urgência que uma pessoa lhe coloca para resolver uma situação fora do normal;
>
> Desconfie do famoso “sabe com quem está falando”;
>
> Desconfie de pergunta que a princípio não tem muito a ver com sua função ou que a pessoa deveria saber e não perguntar;
>
> Não compartilhe o que não é de interesse dos outros, não conte seus segredos, pois estes (sic) serão suas fraquezas;
>
> Desconfie de vantagens e ganhos pessoais exagerados. (SPANDL, 2016 s/p)

Em todas as fontes pesquisadas o fator humano é descrito como o elo mais fraco da segurança da informação, mesmo assim na grande maioria dos casos não é dada a devida importância para essa área, o que muitas vezes cria vulnerabilidades para as organizações.

> Um dos riscos, objeto da presente pesquisa, está associado à vulnerabilidades dos ambientes virtuais das organizações. Em muitos casos, o atacante nem precisa encontrar vulnerabilidades técnicas, na maioria das vezes o sucesso do ataque é alcançado somente com contribuição humana, considerada o elo mais fraco da segurança. Existe uma ampla variedade de ataques que envolvem Engenharia Social: desde enganar usuários para inserirem seus dados bancários ou até mesmo uma senha de acesso remoto a um sistema de uma organização, até a obtenção de acesso físico às dependências da empresa mediante manipulação de guardas de segurança e

> recepcionistas. Quem é responsável pela Segurança da Informação nas organizações? Na maioria das empresas, existem pessoas responsáveis pela segurança de TI, tais como: firewalls, softwares para detecção de intrusão, antivírus, política de senhas, políticas de Segurança da Informação, treinamento/ conscientização dos usuários, auditoria a sistemas e sistemas de backup. Agrega-se a isso, outras pessoas responsáveis pela segurança física: portarias, recepção e monitoramento via CFTV. Então, quem é que deve pensar sobre os aspectos relacionados às pessoas inseridas na organização relacionadas ou não ao sistema de Segurança da Informação. (MAULAIS, 2016 s/p)

Para Fontes (2006, p. 122): “Evidentemente, as organizações maiores são mais vulneráveis a esse tipo de ação, pois um fraudador poderá sempre utilizar a desculpa de que é um colaborador que está em viagem e precisa de ajuda”.

No livro “A arte de enganar”, Kevin Mitinick e Simon (2003) relatam vários casos de fraudes e ataques causados por hackers que em muitos casos conheciam alguém dentro da empresa atacada, ou apenas se fizeram passar por um funcionário para ter acesso a senhas ou informações sigilosas.

> O *Computer Security Institute*, em sua pesquisa de 2001 sobre os crimes de computadores relatou que 85% das organizações entrevistadas detectaram quebras na segurança dos computadores nos 12 meses anteriores. Esse é um número assustador: apenas 15 entre cem organizações responderam que podiam dizer que não haviam tido uma quebra de segurança durante o ano. Igualmente assustador foi o número de organizações que informaram terem tido prejuízos financeiros devido a quebras na segurança dos computadores: 64%. Bem mais do que metade das organizações havia tido prejuízos financeiros. (MITNICK; SIMON 2003, p. 05)

Spandl (2016 s/p) visa a importância de treinar bem os funcionários e principalmente os fazer entender a importância de serem fundamentais na pratica de privacidade da empresa. “Não existe segurança 100% e jamais existirá! Se utilize do que as pessoas mais prezam em suas vidas: família, dignidade, bens e outras coisas que para o ser humano são de grande valia, e um aliado capacitado e treinado terá”.

Existem algumas técnicas típicas utilizadas pelos engenheiros sócias para conseguirem acesso as informações desejadas, que são descritas por Fontes (2006, p. 121).como:

> Falam com conhecimento - Ao contatar alguém da organização, o engenheiro social fala com propriedade sobre um determinado assunto. Se tiver falando de alguém, cita nomes com familiaridade e diz que é parente, ex-colega ou colega atual (no caso de uma grande organização). Pode citar também departamentos e locais da organização, e, se tiver acesso à linguagem utilizada exclusivamente no local, pode alcançar seus objetivos facilmente.
>
> Adquirem a confiança do interlocutor - Com tantas informações citadas no item anterior, o interlocutor pensa que o engenheiro social é uma pessoa de confiança. Muitas vezes o fraudador não tem pressa e volta a telefonar em outra ocasião. A primeira ligação serve apenas para criar um canal de comunicação e estabelecer uma relação de confiança. Com o tempo, cria-se um vinculo entre o fraudador e a vítima.
>
> Prestam favores – Em casos de golpes e fraudes, o engenheiro social pode até ajudar a vítima. O fraudador pode bloquear a comunicação do computador do interlocutor e se passar por alguém do *help desk,* ajudando a resolver um problema que ele próprio planejou. Dessa forma, o interlocutor passa a confiar nele.

Kevin e Simon (2006, p. 76) apresentam o ponto de vista dos hackers e invasores, que muitas vezes se utilizam de seu conhecimento para fazerem roubos milionários ou causar estragos gigantescos em grandes empresas, ou até mesmo se apossarem de informações confidenciais a fim de vendê-las para pessoas interessadas. Em outros casos existem aqueles que invadem por curiosidade, para saberem o que conseguem fazer, até onde conseguem chegar, e ainda, para ostentarem seus feitos em fóruns onde tem contatos com outros hackers. Em muitos casos esses invasores afirmam que não queriam causar mal algum, ou ainda, que não ocasionaram nenhum dano para ninguém, pois suas ações tiveram efeitos mínimos para os afetados.

> Parece espantoso, no mundo de hoje, os hackers ainda acharem tão fácil entrar em sites Web de tantas organizações. Com todas as histórias de invasões, com toda a preocupação com a segurança, com pessoal dedicado, profissionais na equipe ou consultoria disponível a grandes e pequenas empresas, é espantoso que esses dois adolescentes tenham sido suficientemente hábeis para descobrir um modo de entrar nos computadores de um tribunal federal, de uma importante cadeia de hotéis e da *Boeing Aircraft*.
>
> Isso acontece, em parte, acredito, porque muitos hackers seguem o caminho que segui, dedicando um tempo fora do comum ao aprendizado de sistemas de computador, software de sistema operacional, programas de aplicativos, networking e coisas do tipo.

> Eles são, na maioria, autodidatas, mas em parte também são orientados por uma rede informal, mas altamente efetiva, de tutoria, na qual "os conhecimentos são compartilhados". Alguns que mal saíram do ensino fundamental dedicaram tempo e adquiriram conhecimentos suficientes na área para se qualificar a um diploma de bacharel em ciências em *hacking*.

Para Dawel (2005, p. 56). “A questão da engenharia social precisa ser tratada dentro do programa de segurança da informação de qualquer empresa, a fim de conscientizar cada pessoa, funcionário ou terceiro de suas implicações”.

Ainda Kevin e Simon (2006, p. 96) expõem que muitas empresas não levam a sério o fato de estarem vulneráveis e não acham necessário fazer investimentos para melhorar sua área de segurança da informação. Em alguns casos descritos no livro, os hackers se apresentam a empresa que foi vitima de sua invasão para lhes mostrar os riscos que estão correndo e as melhorias necessárias para estarem seguras, mas estas ignoram os avisos.

> Graças à minha experiência pessoal, sei como os promotores aumentam o preço suposto em casos de hacker. Uma estratégia é obter declarações de empresas que superestimam suas perdas na esperança de que o hacker seja declarado infrator em vez de ir a julgamento. O advogado de defesa e o promotor, então, chegam a um acordo quanto a uma soma menor, como a perda que será apresentada ao juiz; sob as diretrizes federais, quanto maior for a perda, mais longa será a sentença.
>
> No caso de Adrian, o U. S. Attorney preferiu ignorar o fato de que as empresas tinham conhecimento de que eram vulneráveis a ataques — porque o próprio Adrian lhes contou isso. Todas as vezes, ele protegeu as empresas avisando-as sobre furos em seus sistemas e esperando até que os problemas fossem corrigidos antes que notícias sobre a invasão fossem divulgadas. Sem dúvida, ele tinha violado a lei, mas agiu eticamente.

1.2.1 Se defendendo de um engenheiro social

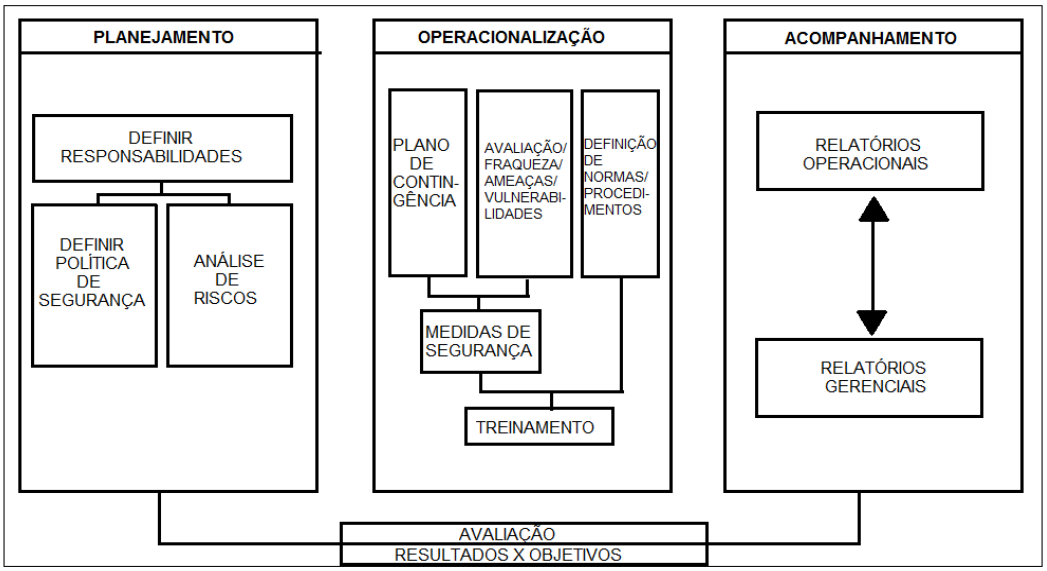
Um dos contra-ataques mais eficazes para proteger a empresa de um engenheiro social é a criação de uma política de segurança rigorosa, com treinamentos e informações que visem deixar a empresa mais segura, com foco, principalmente, no controle aos acessos de pessoas estranhas ou mesmo funcionários não autorizados. Para Ferreira e Araújo (2008, p.36) “A política de segurança define o conjunto de normas, métodos e procedimentos utilizados para a

manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação". E concluem "Deve-se utilizar uma visão metódica, criteriosa e técnica em seu desenvolvimento e elaboração, de forma que possam ser sugeridas alterações na configuração de equipamentos, na escolha de tecnologia, na definição de responsabilidades e, por fim, na elaboração das políticas com o perfil da empresa e dos negócios que ela pratica".

Já para Caruso e Steffen (2006, p.26): "Por política de segurança entende-se política elaborada, implantada e em continuo processo de revisão, valida para toda a organização, com regras (...) claras e simples [...]" e, o fundamental, que a alta gerencia respeite e de suporte a essa política.

Na figura 3 pode-se observar fatores que formam o ciclo da administração de segurança empresarial.

Figura 3: Ciclo da administração de segurança empresarial:



Fonte: GIL (1998, p.15).

Gil (1998, p.33) acredita que: "Para o estabelecimento e verificação da segurança é necessária a determinação de um ponto crítico no ambiente de informática, que mereça acompanhamento para serem evitadas ameaças em relação a erros, omissões, falhas, fraude e roubo".

Caruso e Steffen (2006, p.57) destacam que a política de segurança deve ter diretrizes claras em pelo menos nos seguintes itens:

Objetivos de segurança – deve explicar de forma rápida e sucinta a finalidades da política de segurança.

A quem se destina – deve definir claramente quais as estruturas organizacionais e os ocupantes de funções aos quais a política se aplica.

Propriedade de recursos – deve definir de forma clara quais tipos de responsabilidades envolvidas com o manuseio de ativos de informações, a quem ele deve ser atribuído e quais os mecanismos de transferência.

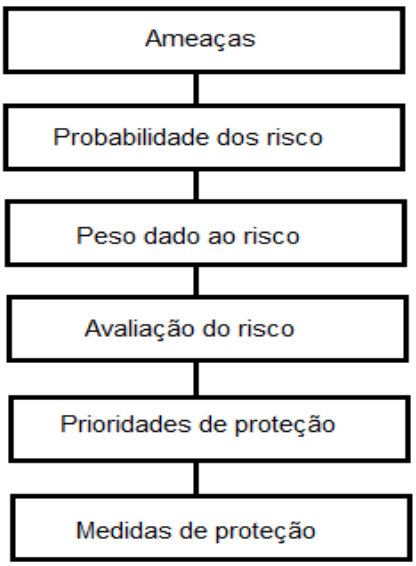
Requisitos de acesso – deve indicar de forma clara quais os requisitos a serem atendidos para o acesso a ativos de informações.

Responsabilização – deve indicar as medidas a serem tomas nos casos de infringências às normas.

Generalidades – nesta seção da política podem ser incluídos os aspectos que não cabem nas demais. Pode-se incluir aqui uma definição dos conceitos envolvidos, um glossário e uma indicação das normas acessórias.

A figura 4 apresenta um fluxograma com a análise das principais ameaças e riscos

Figura 4: Fluxo de análise de ameaças e riscos:



Fonte: CARUSO e STEFEN (2006, p.73).

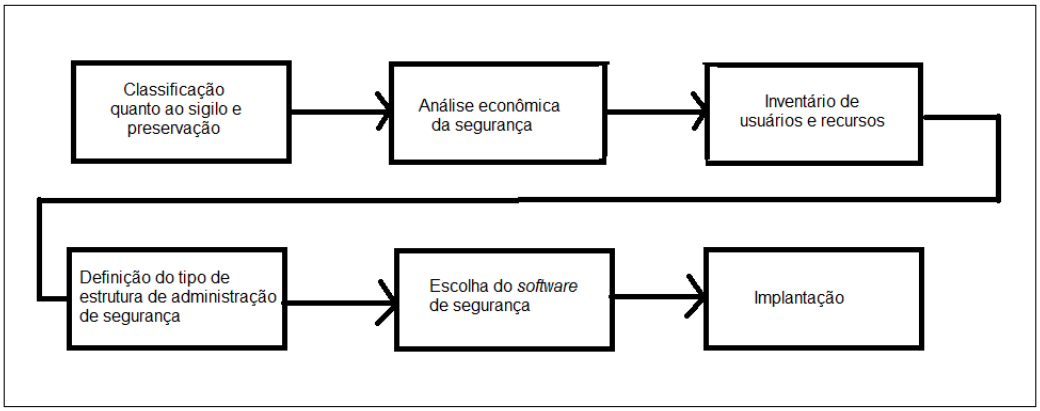
Gil (1998, p.16), instrui: “A política será efetiva, se for comunicada a todos com ênfase adequada. Cada executivo/gestor deve ser incentivado a mostrar

evidências sólidas de implantação das políticas de segurança em sua área de responsabilidade”.

> É preciso, antes de mais nada, cercar ao ambiente de informações com medidas que garantam sua segurança efetiva a um custo aceitável, visto ser impossível obter-se segurança absoluta, já que a partir de determinado nível os custos envolvidos com segurança tornam-se cada vez mais onerosos, superando os benefícios obtidos. Essas medidas devem estar claramente descritas na política global de segurança da organização, delineando as responsabilidades de cada grau de hierarquia e o grau de delegação de autoridade, e, muito importante, estar claramente apoiadas pela alta direção. (CARUSO e STEFFEN 2006, p.24)

Na figura 5 é possível observar as etapas de implantação da segurança.

Figura 5: Sequência das etapas de implantação da segurança:



Fonte: CARUSO e STEFEN (2006, p.64).

Um dos aspectos mais importantes para que a informação se mantenha segura é a identificação do usuário que a está acessando, isso serve para evitar que pessoas mal-intencionadas possam ter acesso à informações confidenciais.

> A identificação informa ao ambiente computacional quem é a pessoa que esta acessando a informação. Ela acontece por meio de seu nome, de seu número de matricula na organização, de seu CPF ou de qualquer outra sequência de caracteres que represente você como usuário. A autenticação tem por objetivo garantir que o usuário descrito na identificação é verdadeiramente essa pessoa. Isto é, busca provar que você é você. (FONTES, 2006 p.24)

Gil (1998, p.76), fala sobre a importância do controle de acesso físico da empresa: “É um processo pelo qual é dada permissão, ou são estabelecidas limitações, a pessoa em seu direito de acesso a áreas ou objetos específicos do tipo, ambiente de informática, plataformas de computação, terminais, arquivos”.

> O controle de acesso físico tem por objetivo a segurança do acesso às áreas delimitadas, edifícios, sala de computadores e de arquivos, centrais de instalações e equipamentos auxiliares. Cada tipo de organização deve levar em conta o grau de risco a que esta exposta quanto a dados, equipamentos e recursos, quando do projeto de instalação destinadas ao processamento de informações. (CARUSO e STEFFEN 2006, p.57)

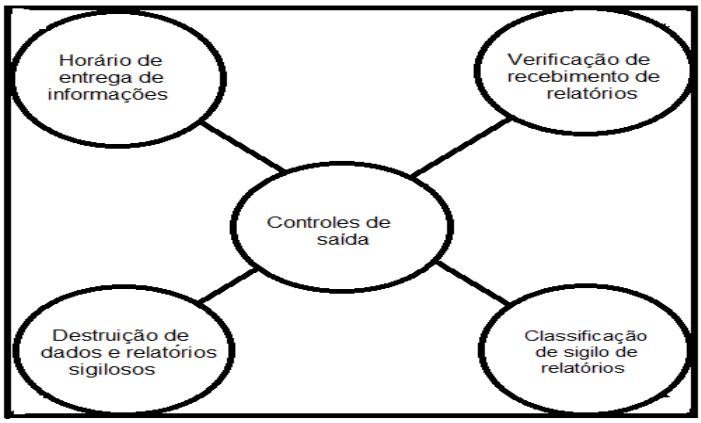
Por muitas vezes haver uma grande preocupação na entrada de pessoas desconhecidas, mas não ser dada a devida importância na hora da saída do individuo Gil (1998, p.77), diz: “[...] Uma alternativa é manter o documento do visitante na portaria para controle mais efetivo de sua saída. Como o visitante vai sozinho ao local da visita, no trajeto tem oportunidade de acessar outros ativos da empresa”.

As políticas não devem se restringir apenas ao ambiente da empresa, mas ao funcionário em si. Em casos de *home office* devem ser criadas normas específicas para o acesso remoto, pois o computador do empregado se torna parte da empresa quando conectado.

> [...] Um funcionário que acessa s rede da empresa de sua residência, devidamente autorizado a isso, está no ambiente externo ou interno? As tecnologias disponíveis permitem a uma pessoa a partir de qualquer computador ligado a Internet, acessar a rede da empresa como se estivesse sentado na sua mesa de trabalho dentro da empresa. Permitem também acessos remotos a central telefônica da empresa, não só para ouvir os recados, mas também para acessar uma linha externa e ligar para qualquer lugar que o seu perfil de usuário permita. DAWEL (2005, p. 25).

Na figura 6 são apresentados fatores importantes para o controle em operações e saídas de informação.

Figura 6: Controle em operações e saídas de informações.



Fonte: GIL (1998, p.128).

Caruso e Steffen (2006, p.27), complementam: “Não existe política de segurança certa ou errada” e muito menos pronta para o uso. “Cada empresa deve ter uma solução única e adequada para o seu caso, para sua cultura”.

2 ESTUDO DE CASO

Nesse capítulo é apresentado o estudo de caso, os dados são demonstrados através de gráficos e, há uma análise das respostas dos sujeitos da pesquisa.

2.1 IDENTIFICAÇÃO DA POPULAÇÃO E INSTRUMENTO UTILIZADO

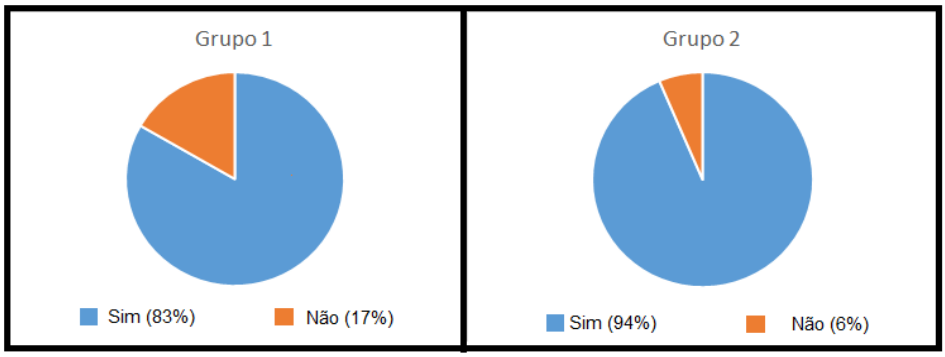
Para realizar o estudo de caso, foi aplicado um questionário (apêndice 1) em 49 alunos do curso Superior de Tecnologia em Segurança da Informação do período noturno da FATEC Americana que trabalham ou trabalharam na área de T.I., com o intuito de saber, primeiramente, se tinham conhecimento sobre engenharia social e se acreditavam que a empresa com a qual se relacionam e/ou relacionou está protegida de ataques de engenheiras sociais. Outro ponto levantado foi se estes alunos já presenciaram uma entrada não autorizada na empresa onde trabalham e como reagiram.

Uma das questões mais importantes levantada foi sobre a política de segurança da empresa, se existe e, principalmente, pelo aluno pesquisado e se recebe bons exemplos de seus superiores.

As perguntas fundamentais para o estudo foram: o grau de segurança de dados sigilosos da empresa, segundo a opinião dos alunos pesquisados, e se estes alunos passariam uma informação para alguém que não tivessem certeza da autorização para acessá-la.

Para analisar os dados, foram separados os respondentes do primeiro ao terceiro semestre que será chamado de Grupo 1 e do quarto ao sexto semestres Grupo 2 respectivamente. O objetivo foi mensurar o conhecimento que os grupos têm sobre engenharia social e política de segurança da informação.

Gráfico 1: Conhecimento sobre engenharia social

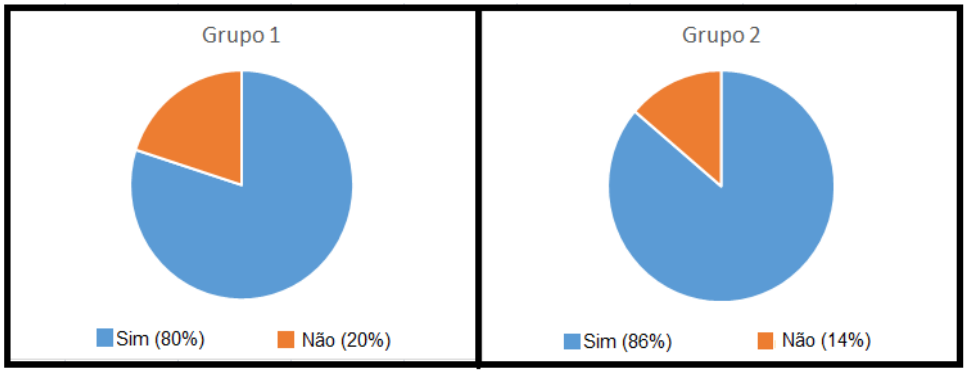


Fonte: Desenvolvido pelo autor.

A partir do gráfico 1 pode-se perceber que a maioria dos alunos do grupo 1 tem conhecimento sobre engenharia social apesar de o assunto não ser muito abordado na grade curricular nos três primeiros semestre do curso. Já no grupo 2, o ideal seria que todos os alunos soubessem sobre o tema, uma vez que ele é abordado exaustivamente a partir do quarto semestre ate o final do curso em várias disciplinas.

Para os sujeitos da pesquisa que disseram saber o que é engenharia social, foi acrescida outra questão como segue abaixo.

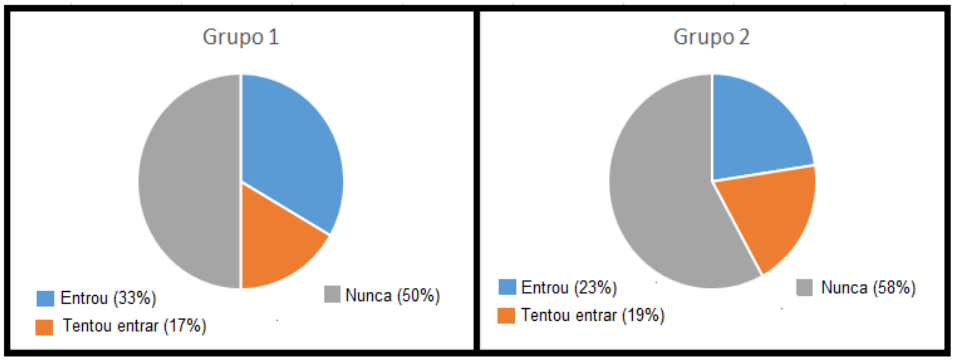
Gráfico 2: A empresa na qual trabalha tem abertura para um ataque de engenharia social.



Fonte: Desenvolvido pelo autor.

Segundo diversos os autores estudados nesse trabalho nenhuma empresa é 100% segura. No gráfico 2 pode-se observar que os alunos dos dois grupos, na maioria, entendem as aberturas que podem ser usadas por engenheiros sociais para realizar Invasões e percebem as janelas existentes nos sistemas utilizados nas empresas onde trabalham ou trabalharam.

Gráfico 3: História que conhecem de tentativa de entrada não autorizada na empresa.

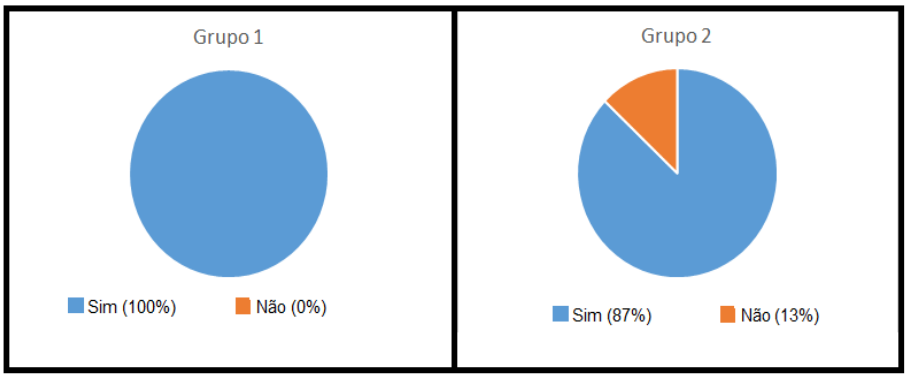


Fonte: Desenvolvido pelo autor.

No gráfico 3 é possível perceber que 50% do grupo 1 e que 42% do grupo 2 sabem de entradas de estranhos ou tentativas de entrar na empresa onde trabalham/trabalharam, o que mostra que muitos invasores não utilizam apenas as redes para tentar conseguir acesso a informações confidenciais, além de mostrar a importância da segurança da informação de modo físico. Mitinik (2003), diz que quebrar a "*firewall* humana" é quase sempre mais fácil do que conseguir invadir uma rede, o que explica a quantidade de tentativas de invasão física.

Ao serem perguntados sobre a reação que tiveram, os que já trabalhavam na empresa pertencentes ao grupo 1, 44% disseram que ficaram preocupados, 44% foram evasivos dizendo apenas que não trabalham mais na organização, agora 11% ficou indiferente, e, no grupo 2 foram 23% fato inesperado aos pesquisadores, pois tal atitude que não faz parte do perfil profissional esperado para um Tecnólogo em Segurança da Informação

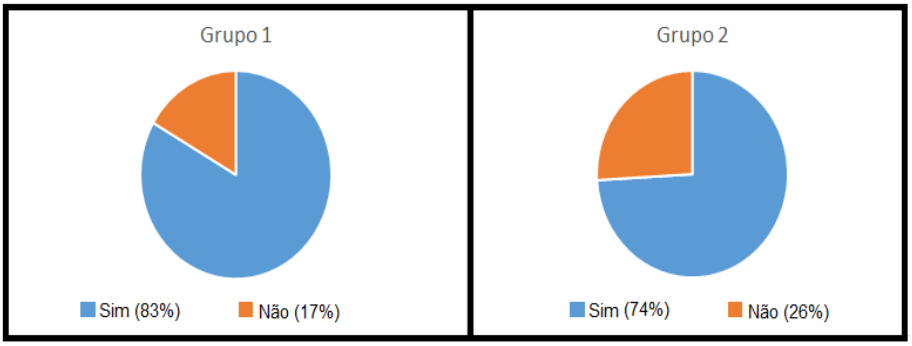
Gráfico 4: Existência de política de segurança onde trabalha.



Fonte: Desenvolvido pelo autor.

Como citado por Caruso e Steffen (2006), uma das proteções mais eficientes contra ataques de engenharia social é a política de segurança de uma organização. No gráfico 4 se pode perceber que ainda existem empresas que não possuem uma política de segurança, algo que seria fundamental, principalmente para as empresas de T.I., onde quase todos os funcionários possuem acesso pelo menos a um computador, podendo acessar muitas informações da empresa.

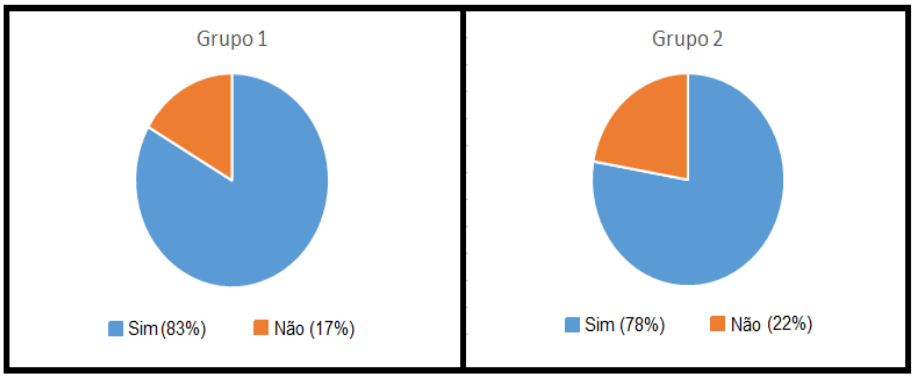
Gráfico 5: Cumprimento da política de segurança onde trabalha.



Fonte: Desenvolvido pelo autor.

No gráfico 5 pode-se observar que a maioria dos sujeitos que trabalham/trabalharam em empresas que possuem uma política de segurança, cumprem essa política minimamente, mas existe uma parcela que não se apegam a essas políticas como deveriam. Isso cria abertura para que pessoas mal intencionadas possam conseguir informações confidenciais da empresa. Como Dawel (2005), ressalta que, todos os funcionários precisam entender o seu papel dentro da empresa e as consequências de seus atos. A importância da política de segurança, assim como os riscos da engenharia social, são abordados e estudados minuciosamente ao longo do curso, entretanto os alunos respondentes demonstram negligenciar esse conhecimento não pondo em pratica o que aprenderam. Isso mostra que eles não têm consciência de sua relevância para o bom andamento do cotidiano de seu trabalho.

Gráfico 6: Cumprimento da política de segurança pelos superiores.

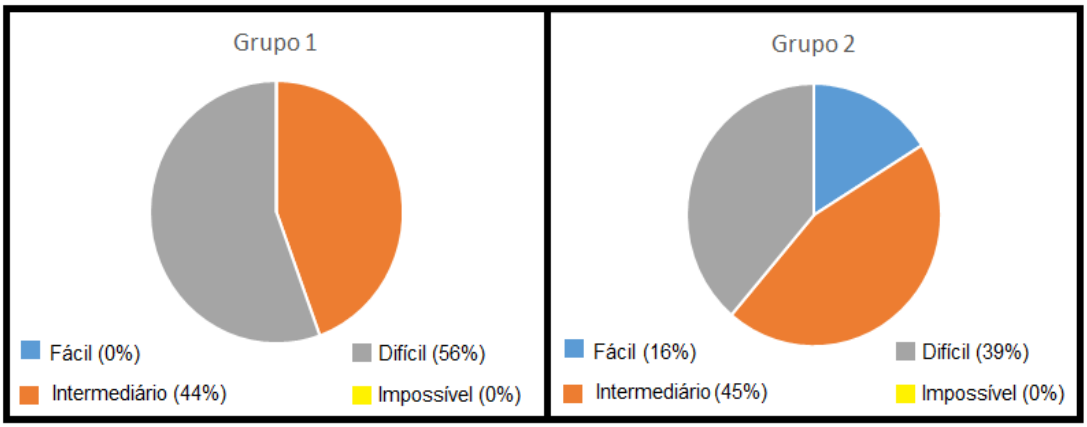


Fonte: Desenvolvido pelo autor.

Como citado por Fontes (2006), muitas vezes, os próprios executivos não dão a importância devida para a segurança da informação, conversam sobre assuntos confidencias sem prestarem atenção no ambiente que estão e descartam papeis com esboços ou ideias sigilosas em locais impróprios, muitas vezes, jogando-os em lixos públicos, como por exemplo, de lanchonetes ou cafés.

O gráfico 6 semelha-se com o gráfico 5, no que tange aos superiores, pois indicam o que indica que quando os superiores também a displicência dos mesmos que não cumprem a política de segurança da empresa, dando péssimo exemplo aos funcionários, esses tendem a não ver a importância da mesma, o que criar vulnerabilidades para a organização. Além de ser presumível que pessoas com cargos superiores têm acesso a informações mais importantes e mais sigilosas, tendo assim que ter maior cuidado.

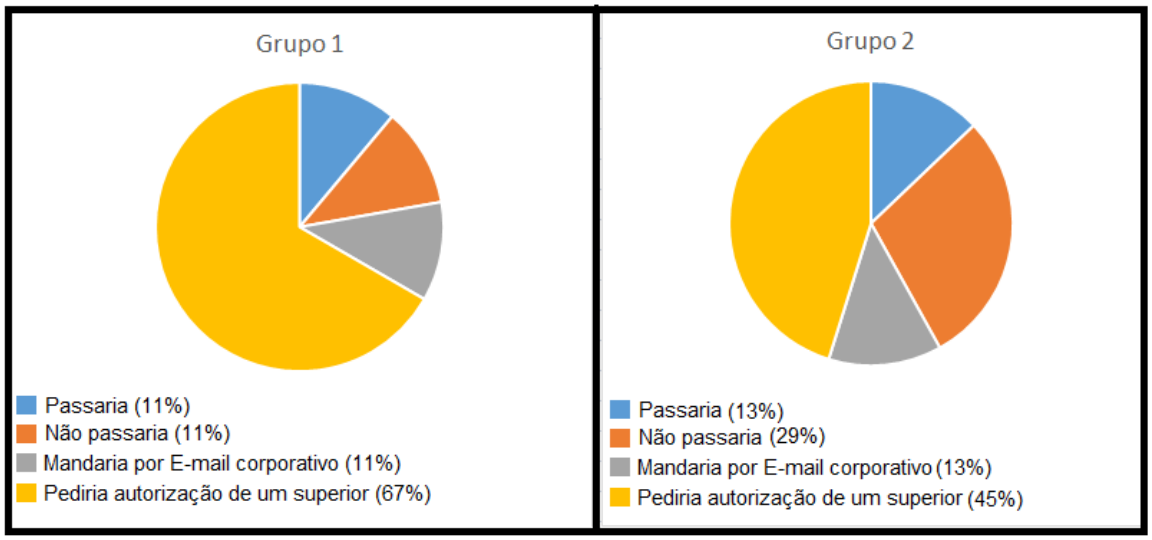
Gráfico 7: dificuldade para conseguir informações sigilosas na empresa, sem a devida autorização.



Fonte: Desenvolvido pelo autor.

Para Mitinik (2003), não importa o quanto a empresa invista em segurança, pois apenas diminui as chances de uma invasão, mas, nunca consegue acabar com todas as vulnerabilidades e que acreditar no contrario cria uma falsa sensação de segurança, que acaba sendo pior que não ter medida de segurança nenhuma. No gráfico 7 é demonstrada a opinião dos sujeitos em relação as empresas onde trabalham ou trabalharam, mostrando a dificuldade para conseguir uma informação na organização sem ter a devida autorização. O grupo 1, mesmo tendo alunos ingressantes, já entende que nunca é impossível conseguir essas informações, mas nenhum desses alunos considerou fácil conseguir esses dados. No segundo grupo já existe uma parcela que considera que conseguir as informações sem a devida autorização é fácil em suas empresas, o que pode indicar que os alunos que estão cursando a partir do quarto semestre já conseguem identificar aberturas para invasão com mais facilidade.

Gráfico 8: Passaria uma informação de caráter sigilosa para uma pessoa que ele não tem certeza que tem a devida autorização.



Fonte: Desenvolvido pelo autor.

Para o desenvolvimento do gráfico 8 foi feita uma pergunta para os respondentes, para conhecer suas reações a um possível ataque de engenharia social. Ambos os grupos responderam que pediriam autorização para um superior para passar os dados solicitados, alguns prefeririam mandar um e-mail corporativo para garantir que a pessoa que pedia a informação realmente trabalhava para a empresa e alguns responderam que não passariam. O ponto alarmante é que, em ambos os grupos, mais de 10% responderam que passariam a informação, estes

deram como justificativa que tinham medo de receberem uma advertência ou causar algum constrangimento para seus superiores. Como citado por Fontes (2006), é sempre melhor pegar as informações de quem esta solicitando a informação e passar para alguém da empresa que tenha certeza se esta pessoa pode ter acesso ao dado solicitado.

3 CONSIDERAÇÕES FINAIS

Com o estudo realizado, é possível perceber que mesmo existindo relatos de invasão a empresas por meio da engenharia social, o tema ainda não recebe a devida importância e que muitas organizações acabam abrindo espaço para esse tipo de ataque, exatamente por acreditarem estarem imunes aos engenheiros sociais. Além de muitas empresas não assumirem publicamente terem sido invadidas por esse método, por medo de expor suas vulnerabilidades.

A partir da apresentação e análise dos dados, observamos que, existem empresas que ainda não possuem uma política de segurança para proteger suas informações, o que, segundo os autores estudados, é a melhor forma de se defender de hackers e engenheiros sociais, por criar regras que definem as pessoas autorizadas a acessar as informações sigilosas da empresa, além de determinar métodos para proteger a rede de invasores e limitar o acesso físico a organização.

Outra questão importante diz respeito ao número de alunos, principalmente os que estão nos últimos semestres do curso, que mesmo mostrando que conseguem perceber as aberturas existentes na empresa para ataques de engenharia social, e tendo como foco principal da grade curricular a proteção das informações, ainda apresentam atitudes que podem prejudicar a empresa em que trabalham por não entenderem ou não se importarem com as consequências dos seus atos.

Uma hipótese que pode explicar esse comportamento dos alunos é a falta de exemplos de funcionários com cargos superiores, que mesmo tendo acesso a informações extremamente sigilosas, muitas vezes acessam ou comentam sobre elas perto de pessoas não autorizadas, ou em ambientes não seguros. Até mesmo o descarte de documentos com as informações da empresa, de seus clientes e funcionários é feito de maneira incorreta, sem dar importância aos dados contidos nesses papéis. Isso pode fazer com que os alunos pesquisados não ponham em prática os conhecimentos de segurança que são apresentados ao longo do curso em todos os semestres.

Infelizmente, ao analisarmos os gráficos, percebemos que não houve a diferença esperada entre os grupos de alunos do curso de segurança da informação do período noturno, pois se esperava que os alunos do segundo grupo (quarto ao sexto semestre) apresentassem independente do comportamento dos outros funcionários, um entendimento maior da importância das regras de segurança e,

principalmente, uma conduta esperada de um profissional que preza, acima de tudo, pela integridade e segurança da empresa.

O objetivo geral foi atingido, pois através do trabalho pode-se identificar diversos riscos que a engenharia social pode apresentar para todas as empresas de T.I.. Além de apresentar as principais características e os principais métodos utilizados por engenheiros sociais e mostrar as consequências de ataques de engenharia social, realizada por estranhos, funcionários e ex-funcionários descontentes.

A hipótese verdadeira foi a “b”. Existiu certa dificuldade para encontrar material confiável e não houve tantos indivíduos para responder o questionário quanto desejado, além de não existirem muitos casos de invasão por meio da engenharia social divulgados recentemente sobre empresas conhecidas, por a maioria tentar evitar a divulgação desse tipo de acontecimento.

A justificativa provou-se correta a partir do estudo feito no primeiro capitulo, onde os autores utilizados ressaltam que realmente as empresas não tomam as devidas providências para evitar os ataques de engenharia social, na grande maioria das vezes por acreditar que não existe abertura dentro da organização para esse tipo de ataque e, principalmente, por confiar que seus funcionários são incapazes de passar informações sigilosas para pessoas não autorizadas, seja por falta de preparo ou para conseguirem algo em troca.

As informações contidas nesse estudo podem ser utilizadas para apontar vulnerabilidades existentes em empresas de T.I., mostrando aberturas para ataques físicos e/ou pela rede através da observação da política de segurança e da cultura organizacional.

REFERÊNCIAS

ARRUDA, Felipe. **Engenharia Social:** o malware mais antigo do mundo. (2011). Disponível em: <https://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm>. Acesso em: 09 nov. 2017.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e segurança da informação.** 3. ed. São Paulo: Senac, 2006. p.23-76.

CASSA, Mônica. **A importância e a implementação da segurança da informação no âmbito das atividades de negócios.** (2013). Disponível em: <http:// www.techoje. com.br/site/techoje/categoria/detalhe_artigo/221>. Acesso em: 30 out. 2017.

CHEHUEN NETO, José Antonio. **Metodologia da pesquisa científica.** Curitiba: CRV, 2012. p.102-103.

CIPOLI, Pedro. **O que é Engenharia Social?** (2014). Disponível em: <https:// canaltech.com.br/segurança/O-que-e-Engenharia-Social/>. Acesso em: 30 out. 2017.

CONCEITO.DE. **Conceito de segurança. (**2011). Disponível em: <https:// conceito.de /seguranca>. Acesso em: 27 mar. 2018.

DAWEL, George. **A segurança da informação nas empresas:** Ampliando horizontes além da tecnologia. Rio de Janeiro: Ciência Moderna, 2005. p.18-56; 102.

DICIO (Brasil). **Dicionário Online de Português:** Hackers: Significado. Disponível em: <https://www.dicio.com.br/hacker/>. Acesso em: 09 maio 2018.

FERREIRA, Fernando Nicolau Freitas; ARAUJO, Márcio Tadeu de. **Política de Segurança da informação:** Guia prático para Elaboração. 2. ed. Rio de Janeiro: Ciência Moderna, 2008. p.07-36.

FONTES, Edison; CISM; CISA. **Segurança da informação:** O usuário faz a diferença. São Paulo: Saraiva, 2006. p.02-122.

GIL, Antonio de Loureiro. **Segurança em informática:** Ambientes mainframe e de microinformática segurança empresarial e patrimonial 200 questões sobre segurança. 2. ed. São Paulo: Atlas S.a, 1998. p.16-37; 76-128.

LAUREANO, Marcos AurelioPchek; MORAES, Paulo Eduardo Sobreira. SEGURANÇA COMO ESTRATÉGIA DE GESTÃO DA INFORMAÇÃO. **Economia & Tecnologia**, Paraná, v. 8, n. 3, p.38-44, maio 2005. Trimestral.

LONG, Johnny. **Google Hacking:** Para testes de invasão. São Paulo: Digerati Books, 2005.

LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação.** Rio de Janeiro: Ciência Moderna, 2006. p.06.

MAULAIS, Claudio Nunes dos Santos. **ENGENHARIA SOCIAL:** Técnicas e estratégias de defesa em ambientes virtuais vulneráveis. 2016. 79 f. Monografia (Especialização) - Curso de Sistemas de informação e gestão do Conhecimento, Universidade Fumec, Belo Horizonte, 2016.

MARCONDES, José Sergio. **Engenharia Social:** o que é? Conceitos , técnicas e como se proteger. (2017). Disponível em: <https://www.gestaodeseguranca privada.com.br/engenharia-social-o-que-e-conceitos/>. Acesso em: 28 out. 2017.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamento de metodologia científica.** 6. ed. São Paulo: Atlas S.A, 2009. p.75

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamento de metodologia científica.** São Paulo: Atlas S.A, 2012. p.185.

MENEZES, Josué das Chagas. **Gestão de segurança da informação.** Leme: JhMizuno, 2006. p. 26-41.

MITNICK, Kevin D.; SIMON, William L.. **A arte de enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Sao Paulo: Pearson, 2003. 304 p.

MITNICK, Kevin D.; SIMON, William L.. **A ARTE DE INVADIR:** As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. São Paulo: Pearson Prentice Hall, 2006. 236 p.

OLIVEIRA, Jayr Figueiredo de. **Sistemas de informação versus tecnologias da informaçao.** 2. ed. São Paulo: Érica, 2004. p. 23-34.

PEIXOTO, Mario Cesar Pintaudi. **Engenharia social e segurança da informação:** Na Gestão corporativa. Rio de Janeiro: Brasport, 2006. p. 04-20.

RAFAEL, Gustavo de Castro. **Engenharia Social:** as técnicas de ataques mais utilizadas. (2013). Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-técnicas-de-ataques-mais-utilizadas/>. Acesso em: 01 nov. 2017.

RAMPAZZO, Lino. **Metodologia científica:** Para alunos dos cursos de graduação e pós-graduação. Lorena: Stiliano, 1998. p.58

RUFINO, Nelson Murilo de O. **Segurança Nacional:** Técnicas e Ferramentas de Ataque e Defesa de Redes de Computadores. São Paulo: Novatec, 2002. p.26.

SAMPIERI, Roberto Hernández; COLLADO, Carlos Fernández; LUCIO, Pilar Baptista. **Metodologia da pesquisa.** 3. ed. São Paulo: Mc Graw Hill, 2006. p.274.

SISTEMAS DE SEGURANÇA. **Importância da segurança da informação. (**2015). Disponível em: <http://www.sistemasdeseguranca.pt/geral/importancia-da-seguranca-da-informação/>. Acesso em: 30 out. 2017.

SPANDL, Reinhold. **Segurança da Informação|Fator Humano:** abordagem alternativa. (2016). Disponível em: <https://cryptoid.com.br/banco-de-noticias/

seguranca-da-informacao-fator-humano-abordagem-alternativa/>. Acesso em: 29 out. 2017.

APÊNDICE 1

IDADE_____. SEMESTRE_____.

1.Você sabe o que é engenharia social?
( ) Sim ( )Não

Se sim, você acredita a empresa na qual trabalha tem abertura para o ataque de engenharia social?
( ) Sim ( )Não

2. Você sabe de alguma história de tentativa de entrada de estranhos na empresa?
( ) Alguém já entrou ( )Alguém tentou entrar ( )Nunca

Se sim, qual foi a sua reação?
R:_____

3. Na empresa onde trabalha existe uma política de segurança?
( ) Sim ( )Não

Você e seus colegas cumprem, minimamente, as políticas de segurança da empresa?
( ) Sim ( )Não

Os seus superiores cumprem, minimamente, as políticas de segurança da empresa?
( ) Sim ( )Não

4. Você acha que conseguir informações sigilosas na sua empresa, sem a devida autorização é:
( ) Fácil.
( ) intermediário.
( ) Difícil.
( ) Impossível.

5. Alguém te liga dizendo ser um funcionário, um cliente ou até mesmo um gerente da sua empresa e te pede uma informação de caráter sigilo, mas você não reconhece a voz ou o nome dessa pessoa. O que você faria? (UTILIZE O VERSO DA FOLHA SE NECESSÁRIO)

R:_____
_____
_____
_____
_____