FACULDADE DE TECNOLOGIA DE JAHU

CURSO SUPERIOR DE GESTÃO EM TECNOLOGIA DA INFORMAÇÃO

APLICAÇÃO DA POLÍTICA DE SEGRANÇA DA INFORMAÇÃO NA EDUCAÇÃO E MÉTODO DE PREVENÇÃO DA ENGENHARIA SOCIAL EM UMA EMPRESA DA ÁREA HOPITALAR

RAFAEL GODOY

SAMUEL CRISTIANO PARRA

2° SEMESTRE - 2015

JAHU –SP

RAFAEL GODOY
SAMUEL CRISTIANO PARRA

APLICAÇÃO DA POLÍTICA DE SEGRANÇA DA INFORMAÇÃO NA EDUCAÇÃO E MÉTODO DE PREVENÇÃO DA ENGENHARIA SOCIAL EM UMA EMPRESA DA ÁREA HOPITALAR

Monografia apresentada à Faculdade de Tecnologia de Jahu, como parte dos requisitos para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Orientador: Me. Robson Antônio Moreira

2° SEMESTRE - 2015
JAHU – SP

A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original.

Oliver Wendell Holmes Sr

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, e em segundo a minha família e a minha namorada que sempre acreditaram em mim e me deram força para concluir este trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me dar forças; a minha namorada, meus familiares e ao meu professor orientador Me. Robson Antônio Moreira e em especial todos meus amigos que trabalham comigo e que nos ajudaram de diversas maneiras.

DEDICATÓRIA

Ofereço esse trabalho a todos os meus familiares que desenho em meu lar, os quais no momento mais difíceis sempre me deram apoio e me ajudou a conquistar mais está vitória.

AGRADECIMENTOS

Agradeço por este trabalho primeiramente a Deus aos meus familiares a meu orientador e aos professores que nos ajudaram em mais uma vitória

RESUMO

O presente trabalho tem como objetivo principal abordar a engenharia social no que se compete aos seus métodos, técnicas e meios de utilização para ludibriar seus indivíduos alvo e comprometer assim a informação e sua segurança, de maneira que possa haver o tipo de reconhecimento dessa abordagem e não ser mais uma vítima dessa prática comum nos dias atuais. Despertar a conscientização das pessoas e das organizações para esse perigo iminente, pois essa é a melhor maneira de proteger a informação. Conhecer o conceito de engenharia social e segurança da informação, assim como a importância nas organizações, evidenciando algumas características do ser humano que o torna o elo mais fraco da segurança da informação, como também as características e o perfil de engenheiro social, para o seu reconhecimento. Portanto, foi realizado um estudo demonstrado como é realizada a aplicação da política de segurança no combate a engenharia social e quais foram os resultados. Com isso o leitor terá uma visão mais ampla dos riscos, danos e consequências causadas pela engenharia social, assim obtendo os recursos necessários para se proteger.

Palavras-chave: Engenharia Social, Segurança Informação, política de informação

ABSTRACT

The present work has the main objective of approaching the social engineering as it competes to its methods, techniques and means of being used to hoodwink their target individuals and thereby compromises the information and its security, so that you can have the type of recognition of this approach and not being another victim of this common practice nowadays. Raise the awareness of people and organizations to this imminent danger, because this is the best way to protect the information. Knowing the concept of the social engineering and information security, as well as the importance in the organizations, showing some characteristics of the human being who is the weakest link in the information security, as also the characteristics and the profile of the social engineering, to your knowledge. Therefore, a study was conducted in order to show how the application of security policy is held to combat the social engineering and what the results were. With that the reader will have a broader view of the risks, damages and consequences caused by the social engineering, thus obtaining the necessary resources in order to be protected.

Keywords: Social Engineering, Information Security, Information Policy

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

O presente trabalho é sobre a informação, seu valor e de como assegurá-la, porque, atualmente é algo extremamente valioso para as organizações. Por isso, passa a ser alvo de pessoas mal-intencionadas com o objetivo de roubá-las ou danificá-las seja por diversão, benefício próprio, vingança ou descobrir segredos de outras pessoas. Sendo assim, existe uma enorme preocupação com que diz respeito à segurança das informações e de como combater uma possível tentativa de roubo ou fraude nas organizações.

No decorrer desta obra dividida por capítulos, tratará dos tipos de informações, a importância que ela tem para organização, a importância de uma política de segurança bem estruturada, didática e flexível para orientação dos funcionários para que eles possam ter os cuidados e conhecimentos necessários para evitar um ataque de engenheira social.

A questão é que as organizações enfatizam, na maioria das vezes, é somente a atualização de computadores, firewalls, antivírus e etc., em seu parque tecnológico que também é muito importante e fundamental para a segurança da informação, entretanto, não é o suficiente. Infelizmente não adiantará trancar sempre sua casa, manter cadeados ou sistemas de segurança em suas portas, se alguém de dentro poderá abri-las para outra pessoa entrar, o que, colocará todo investimento a baixo.

1. A IMPORTÂNCIA DA INFORMAÇÃO

Atualmente a informação é um dos recursos mais valiosos de uma organização. Esse termo, no entanto, é frequentemente confundido com dados. Para esclarecer a diferença, segundo STAIR, Ralph M.; REYONLDS George W. (2015), os dados são fatos brutos, como quantidade de funcionários, horas trabalhadas, quantidade de vendas e de peças no estoque. Mais quando os dados são organizados de maneira significativa se tornam informações, porque, informações são fatos organizados e processados de modo que tenha valor adicional, que se estende além do valor dos fatos individuais. Trocando em miúdos nada mais é que o resultado de todos os processos, organização e manipulação dos dados a qual representa uma modificação que pode ser quantitativa ou qualitativa, também a informação pode ser definida como um ativo, ou seja, um bem da empresa, que como qualquer outro é essencial para os negócios e merece ser tratado de forma especial com toda a proteção.

Pelos que podemos observar a informação tem um muito valor para a empresa e, também, é um recurso vital, de extrema importância nas tomadas de decisões.

Sendo assim as informações podem ser apresentadas em diversas formas tais como impressas, escritas, armazenadas eletronicamente, mas, possui um ciclo de vida e também ela pode ser tratada de várias formas como, por exemplo:

- Ostensiva: podem ser manuseadas por qualquer pessoa e não possuem conteúdo crítico para a instituição;

- Reservadas: Toda informação cujo conhecimento estará restrito a um grupo de pessoas autorizadas, cuja revelação não permitida possa comprometer planos, operações ou objetivos neles previstos.

- Confidenciais: Toda informação que, caso seja revelada, pode trazer grande impacto ou repercussões negativas ao negócio ou para a imagem da instituição, embaraços administrativos com funcionários ou ainda trazer vantagens a terceiros. Este tipo de informação requer alto grau de controle e proteção contra acessos não autorizados

  .

- Sigilosas: representam informações de conhecimento restrito a uma quantidade reduzida de pessoas autorizadas.

Mas, existem outros significados que definem informação e o seu valor. Dois dos melhores são:

Peixoto (2006) que define informação como:

> "Ato ou efeito de informar ou informar-se; comunicação, indagação ou devassa. Conjunto de conhecimentos sobre alguém ou alguma coisa; conhecimentos obtidos por alguém. Fato ou acontecimento que é levado ao conhecimento de alguém ou de um público através de palavras, sons ou imagens. Elemento de conhecimento suscetível de ser transmitido e conservado graças a um suporte e um código. " (PEIXOTO, 2006, pág. 4)

Enquanto o código de prática para a gestão da segurança da informação diz o seguinte:

> "O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos.
> Ativos são objeto de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes. Mudanças nos processos e sistemas do negócio ou outras mudanças externas (tais como novas leis e regulamentações), podem criar novos riscos de segurança da informação. Desta forma, em função das várias maneiras nas quais as ameaças podem se aproveitarem das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos. (ABNT, 2013, pág. 4).

Ainda, segundo o Código (ABNT, 2013, pág.4) pode-se observar que nas organizações, assim tanto quanto um ativo qualquer, as informações são importantes no processo de apoio a decisão, sustentada em muitos servidores, e através de redes integradas de computadores, confiam às informações a toda sua extensão. E é de suma importância mantê-las protegidas, através de um conjunto de controles incluindo políticas, processos, procedimentos, estruturas organizacionais, funções de software e hardware, tendo em vista, sempre a segurança de informação.

1.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o ele, maximizar o retorno sobre o investimento e as oportunidades de negócio (NBR ISO/IEC 27002:2005).

De acordo com Peixoto (2006) o termo segurança da informação é uma área que salva e protege os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas entre outros.

As organizações normalmente investem muito em sistemas de detecção de intrusos, como antivírus, proteções como firewall e etc.. Elas se preocupam em fechar as portas, mas esquecem de que lá dentro há alguém que pode abri-las, porque não faz parte da cultura das empresas investirem em treinamento e conscientização dos usuários sobre o valor da informação. Porém, de acordo com Mitnick (2003), nem isso é o suficiente:

> "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. "

A segurança da informação é formada por pilares básicos, que se definem da seguinte maneira (ABNT NBR ISO/IEC 17799, 2005):

- Confidencialidade: Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados e analisados criticamente, de forma regular. Considerando os requisitos para proteger as informações confidenciais, usando termos que são obrigados do ponto de vista legal. Para identificar os requisitos para os acordos de confidencialidade ou de não divulgação.

- Integridade: Convém que a integridade das informações disponibilizadas em sistemas publicamente acessíveis seja protegida para prevenir modificações não autorizadas.

Convém, que aplicações, dados e informações adicionais que requeiram um alto nível de integridade e que sejam disponibilizados em sistemas publicamente acessíveis sejam protegidos por mecanismos apropriados, como, por exemplo, assinaturas digitais e que os sistemas acessíveis publicamente sejam testados contra fragilidades e falhas antes da informação estar disponível.

- Disponibilidade: Segundo Peixoto (2006) não adianta a informação possuir integridade e confidencialidade, se ela nunca está disponível. Então, o desafio é manter essa estrutura de trafego de informações possibilitando seu acesso sempre.

- Não repúdio e autenticidade: Ainda, de acordo com a norma é procedimentos para assegurar a rastreabilidade dos eventos, usando, por exemplo, técnicas de criptografia ou autenticação para obter prova e registro da ocorrência ou não ocorrência de um evento ou ação.

A Figura 1 ilustra os pilares básicos descritos acima.

Figura 1 - Os pontos chave da Segurança da Informação.

Fonte: (Mendes, 2004)

Vale ressaltar que as ameaças, podem ser de diversas naturezas e, nesse sentido, geralmente, classificadas como passiva, ativa, maliciosa, não maliciosa. Para lidar com essas ameaças, torna-se necessário a definição de políticas e mecanismos de segurança, visando dar suporte a:

- Prevenção, evitando que invasores violem os mecanismos de segurança como, por exemplo, abrindo portas do firewall;
- Detecção, a habilidade de detectar invasões aos mecanismos de segurança como, por exemplo, antivírus que as detectas e as elimina antes que obtenham sucesso;
- Recuperação, utilizando ferramentas e equipamentos de backup para manter a operacionalidade do sistema caso ocorra invasão ou desastres, e software de monitoramento e antivírus para interromper a ameaça, avaliar e reparar danos.

Os pilares acima revelam três aspectos que, também, envolvem a organização:

- Pessoas: Usuários muito bem orientados, treinados e conscientizados da importância da informação e o seu valor.
- Processos: Regras claras para utilização dos recursos tecnológicos fornecidos pelas organizações e leis que venham punir rigorosamente os infratores caso desviem informações
- Tecnologia: Sistemas bem implementados para garantir a proteção das informações da empresa. (PEIXOTO, 2006)

Dentre estes aspectos podemos dividir a segurança em camadas nas quais serão apresentados na sequência desse trabalho.

1.2 CAMADAS DE SEGURANÇA DA INFORMAÇÃO

A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar

um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada. (SÊMOLA, 2003).

Para Schneider (2001), “as ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados. ” O crime no ciberespaço inclui tudo o que se pode esperar do mundo físico: roubo, extorsão, vandalismo, voyeurismo, exploração, jogos de trapaças, fraude etc.

Para Sêmola (2003), a gestão da segurança da informação pode ser classificada em três aspectos: tecnológicos, físicos e humanos. As organizações preocupam-se principalmente com os aspectos tecnológicos (redes, computadores, vírus, hackers, Internet) e se esquecem dos outros – físicos e humanos – tão importantes e relevantes para a segurança do negócio quanto os aspectos tecnológicos.

Adachi (2004) que estudou a gestão da segurança dividindo-a em três camadas: física, lógica e humana.

1.2.1 Camada física

Nada mais é o local onde o hardware está instalado fisicamente, computadores, servidores e meio de comunicação, que pode ser o escritório da empresa, da fábrica, da residência do usuário que administra todas as informações da empresa, neste caso é feito remotamente.

Para Adachi (2004), “a camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação com seus modems, cabos e a memória física, armazenada em disquetes, fitas ou CDs”.

No caso de pequenas e medias empresas geralmente tem seus dados armazenados em servidores de rede ou estações compartilhadas, tendo o acesso físico a estes equipamentos raramente é restrito, na maioria das empresas o servidor ou a estação tem o seu acesso liberado e ilimitado a internet aumentado então o risco de um incidente de segurança.

Uma solução para gerir esse problema e garantir a segurança desta camada, é ter controle de acesso aos recursos de tecnologia da informação (TI) [1] utilizando de equipamentos para fornecimento ininterrupto de energia e firewalls.

1.2.2 Camada lógica

É nesta camada que o software é utilizado, onde os programas de computadores são responsáveis pela funcionalidade do hardware, pela realização de transações em base de dados organizacionais e criptografia de senhas e mensagens etc.

Segundo Adachi (2004), é nessa camada que estão as “regras, normas, protocolo de comunicação e onde, efetivamente, ocorrem as transações e consultas”.

A segurança, em nível lógico, refere-se ao acesso que indivíduos têm às aplicações residentes em ambientes informatizados, não importando o tipo de aplicação ou o tamanho do computador. As ferramentas de controle são, em sua maior parte, “invisíveis” aos olhos de pessoas externas aos ambientes de informática; estas só os reconhecem quando têm o seu acesso barrado pelo controle de acesso. (CARUSO e STEFFEN, 1999).

Uma forma de minimizar os riscos de segurança nesta camada é sempre manter os softwares atualizados, garantindo assim a segurança da informação.

1.2.3 Camada humana

É nesta camada que se concentram todos os recursos humanos presentes na organização, principalmente os que possuem acesso aos recursos de TI, sejam para manutenção ou uso.

Nesta camada tem alguns aspectos importantes que são: a percepção do risco pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem; são usuários instruídos ou ignorantes no uso da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social (ADACHI, 2004).

Segundo SCHNEIER, (2001), das três camadas, esta é a mais difícil de se avaliar os riscos e gerenciar a segurança, pois envolve o fator humano, com

características psicológicas, socioculturais e emocionais, que variam de forma individual.

A gestão da segurança da informação vai além de apenas gerenciar os recursos de tecnologia, ela envolve também as pessoas, os processos, mas algumas empresas acabam negligenciando este fator, para resolver este problema pode-se aplicar uma política de segurança e conscientizar os usuários de como utilizar os recursos tecnológicos.

2. ENGENHARIA SOCIAL

Segundo Silva (2008) o termo engenharia social ficou mais conhecido em 1990, através de um famoso hacker chamado Kevin Mitnick. Este termo foi atribuído às práticas utilizadas para conseguir informações confidenciais das empresas, pessoas e sistemas de informação, explorando a confiança das pessoas para enganá-las. Pode-se também definir engenharia social como um modo de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para enganar as pessoas.

Schneier (2001) nos traz uma das melhores definições:

> "A engenharia social é o termo de hacker para um jogo de trapaça: persuadir a outra pessoa a fazer o que você deseja. Ela é muito eficiente. A engenharia social evita criptografia, segurança do computador, segurança de rede, e tudo o mais que for tecnológico. "

Schneier (2001) nos mostra que a engenharia social vai diretamente para o elo mais fraco de qualquer sistema de segurança: o ser humano, porque o engenheiro social obterá acesso e/ou toda ajuda que puder obter facilitando assim o seu trabalho.

2.1 PERFIL DO ENGENHEIRO SOCIAL

Segundo Mitnick (2003), o engenheiro social é uma pessoa agradável, sendo assim, educada, afável, cativante. Mas, sobretudo inovadora, flexível e dinâmica. Possuindo uma conversa bem envolvente. Os ataques dos engenheiros sociais são normalmente praticados por Crackers, (hackers mal-intencionados), que possuem a arte de enganar, utilizando técnicas de persuasão e exploração da ingenuidade dos usuários, criando um ambiente psicológico perfeito para seu ataque, como por exemplo, utilizando identificações falsas, carisma e o apelo sentimental a fim de conquistar a confiança da vítima.

Normalmente o engenheiro social procura deixar sua vítima bem tranquila, passando-se por alguém do mesmo nível hierárquico ou superior dentro da organização ou até mesmo por clientes e fornecedores de maneira a induzi-los a fornecer informações, executar programas ou até mesmo fornecer senhas de acesso.

Esses profissionais da arte de enganar podem utilizar como pretexto situações de emergência ou de segurança da empresa e geralmente, não pedem muita informação de uma só vez para a mesma pessoa e sim aos poucos e para pessoas diferentes, para que ninguém desconfie deles.

O mesmo autor continua relatando que o chamado engenheiro social é dotado de um enorme poder de criatividade. Essa criatividade é tão grande que na maioria das vezes, a vítima nem imagina que foi usada e muito menos que acabou de abrir o caminho para um invasor. Para que um ataque de engenharia social seja bem-sucedido, é necessária bastante paciência e persistência e essa é uma das grandes características dos mesmos.

2.2 O FATOR HUMANO

Em qualquer empresa a sua segurança, por maior que seja, sempre haverá um fator de desequilíbrio chamado fator humano. Um dos maiores problemas atualmente na segurança da informação está relacionado ao ser humano. Práticas que permitem o acesso não autorizado a dados, lugares, objetos e entre outros, fragiliza qualquer esquema de segurança da informação, uma vez que as pessoas acabam tendo acesso a informações indevidas, colocando em risco a segurança da informação. Um dos grandes assuntos discutidos atualmente é a questão da inclusão do fator humano e o combate a engenharia social como um dos elementos base da segurança da informação. Existem propostas de modelos para inclusão desse fator primordial como um dos pilares fundamentais da segurança da informação. (MITNICK, 2003)

2.3 TÉCNICAS DE ENGENHARIA SOCIAL

Para obter informações sobre indivíduos, um engenheiro social deve conquistar a confiança ou aquiescência deles. E isso é feito, segundo (BASTA, Afred; BASTA, Nadine; BROWN, Mary) 2014, com o uso das seguintes técnicas descritas de detalhadas abaixo.

- Personificação,
- Suborno,
- Fraude,
- Afinidade,

- Engenharia sócia reversa,
- Introdução física,
- Meios de comunicação
- Correspondência escrita
- E-mail
- Mensagens instantâneas
- Comunicação por telefone

2.3.1 Personificação

A personificação refere-se a técnica da representação pessoal, ou seja, o engenheiro social ou hacker finge ser um funcionário ou usuário legitimo do sistema, e com autoridade, tenta coletar informações.

Como por exemplo:

- Abordar um usuário dizendo ser um administrado do sistema pedindo suas senhas.

- Usar uma vestimenta com o nome da telefônica local ou prestadora de serviço, passando-se por um técnico para entrar na central de fiação trancada ou áreas restritas.

- Dar um telefonema para dizer que o sistema está agindo de forma instável e que a vítima deve autenticar seu nome de usuário e senha para verificação.

- Fingir ser um usuário agitado, em dúvida, mas legitimo, e dar um telefonema para um help desk (suporte) para pedir informações.

- Ligar para um administrador de sistemas de terceiro turno dizendo ser o diretor de TI e pedir para fazer alguma alteração em servidores em linhas de código e etc.

Vale salientar, também, que antes de se envolvem nesse tipo de engenharia social, um hacker faz uma pesquisa sobre a companhia alvo, para evitar quaisquer suspeitas. E que é mais fácil se envolver nesse tipo de personificação em empresas grandes e mais diversificadas geograficamente do que em empresas menores nas quais os funcionários têm maior probabilidade de se conhecer. (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

2.3.2 Suborno

O suborno pode ser uma forma eficiente de se obter informações. Nesse caso, o hacker utiliza da ganância do funcionário contra a lealdade da organização. Depois que o suborno foi aceito, a chantagem é a maneira mais normal para manter o funcionário trabalhando para o hacker. E ao procurar uma vítima, um engenheiro faz a seguintes perguntas sobre os funcionários. BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

- Eles trabalham em um nível da organização que poderia fornecer informações uteis?
- Eles estão passando por problemas financeiros?
- Eles possuem algum vicio como jogo, drogas ou álcool?
- Eles estão descontentes com empresa?
- Eles estão orientados a ganhos a curto prazo na empresa?
- Eles são moralmente corruptíveis?

O suborno é uma técnica que exige tempo e muita pesquisa em um indivíduo alvo. Há também um problema relativamente caro a se levar em consideração. Porque durante a pesquisa, o hacker possivelmente terá de investir tempo e recursos na (s) pessoa (s) que está (ão) sendo subornada (s).

O maior risco do suborno é o funcionário, apesar de pronto desejoso de aceitar, seja incapaz de oferecer qualquer informação útil ou mude de ideia, antes ou depois de concluída essa etapa do plano. (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

2.3.3 Fraude

"A fraude envolve, na verdade entrar na empresa como funcionário ou consultor. Isso coloca o hacker "virtuoso" contra a empresa "maligna" e exige uma boa dose de auto ilusão por parte do hacker. "

2.3.4 Afinidade

Ainda, segundo, (BASTA, Afred; BASTA, Nadine; BROWN, Mary) 2014 esse método irá depender da tendência que as pessoas têm de acreditar serem "parecidas", ou seja, existindo uma similaridade aparente entre elas e outas pessoas que na casa sejam desconhecidas. O hacker poderá usar dessa sensação de afinidade para convencer as vítimas de que elas têm muito em comum entre si e compartilhando os mesmos valores. Estabelecer essa sensação de harmonia é um recurso para ganhar a confiança da vítima. E quando a informação necessária for obtida, o hacker certamente se afastará. Essa é uma outra área que um hacker ético pode escolher seguir como parte de um teste de invasão combinado, mas, neste caso, deve ser feito com o conhecimento de que os que são alvo poderem se sentir vitimados, independentemente de o hacker ético não ter más intenções.

2.3.5 Engenharia social reversa

Engenharia social reversa é uma operação trapaceira na qual o hacker finge ser uma autoridade que poderá resolver os problemas das pessoas. Mais a questão é que os problemas são causados pelo próprio hacker da maneira descrita abaixo.

1. Primeiro o hacker cria um problema, por exemplo, como um ataque na negação do serviço (DoS) que paralisa a rede por um tempo.

2. Depois, o hacker se apresenta como um especialista que pode resolver esse tipo de problema. A vítima poderia ser induzida a se comunicar com o hacker em busca de ajuda, o qual aproveita a oportunidade para resolver o problema dela.

3. Agora se acredita que o hacker seja um auxiliar ou especialista de confiança na área de segurança de redes, e assim, recebendo mais acesso à rede em questão incluída muitos sistemas.

4. E por fim o hacker é capaz de obter informações de usuários talvez instalar processos ocultos, para executar em sistemas aos quais tem acesso agora.

Muitos ataques de engenharia social são oportunistas; o hacker usa técnica que considerar mais adequada para a situação, mais todas as técnicas de engenharia social são afetadas pela facilidade da entrada física na organização-alvo ou de comunicação com as vítimas dentro da organização. BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

2.3.6 Intrusão física

Introdução física refere-se a engenheiros sociais que tem acesso dentro das instalações da organização com um único propósito de coletar informações. A intrusão física resulta no usa da personificação ou formas de disseminação para obter acesso a áreas nas quais a entrada do hacker não deveria ser permitida.

Primeiro o engenheiro social deve avaliar a instalações que em geral inclui:

- Aprender os horários da empresa;

- Conhecer a planta do (s) Edifício;

- Fazer vigilância ou pesquisa para compreender os procedimentos de segurança.

Aprender os horários ou os padrões da organização inclui que pessoas estarão lá em que momentos, suas atividades e seus estilos de vida. Também é interessante saber, quem fica com as chaves e onde as pessoas costumam frequentar em vários períodos do dia. Quanto mais o hacker souber a respeito do comportamento dos funcionários, menos levantarão suspeitas. (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

Vale salientar, também, que falhas na segurança das plantas do edifício podem oferecer ao hacker oportunidade de chegar a um lugar certo rapidamente sem muita dificuldade.

Conhecer medidas de segurança que estão sendo usadas também ajuda os hackers, a saber, que ponto o sistema se segurança falha, porque assim que o hacker adquire informações sobre a empresa, ele poderá confeccionar até crachás de identificação falsa.

O último passo é adquirir dados uteis através do desenvolvimento de uma sequência viável de ações, o hacker pode ser capaz de passar um bom tempo desacompanhado no edifício, sobre o qual ele adquiriu toda informação. A essa altura, ele pode ter colocado *Keyloggers* (software ou hardware que rouba senhas) ou ter arrombado fechaduras de gavetas, armários ou arquivos abertos, procurando por documentos de negócios ou senhas de usuários que as escrevem e deixam a vista ou até mesmo observando um usuário ao digitar.

Mais quando a intrusão física não é possível ou não se teve toda informação necessária os hackers usam, às vezes, os meios de comunicação para exercer suas atividades de maneira mais sigilosas e causar menos suspeitas.

2.4 INTRUSÃO FÍSICA

Engenheiros sociais usam correspondência escrita, e-mail, mensagem instantânea, rede sociais e telefone para obter informações úteis de indivíduos-alvo

este trabalho traz uma breve visão geral desses vários meios. (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

(RALPH M. STAIR; GEORGE W. REYONLDS) 2015

2.5 CORRESPONDÊNCIA ESCRITA

Um dos meios de comunicação mais respeitados, o correio convencional se trata de uma ferramenta poderosa para engenheiros sociais obterem dados pessoais sobre usuários. Em um ataque típico, a vítima recebe uma carta dizendo que ganhou um prêmio. O conteúdo da correspondência e elegante e profissional, mais, solicitando detalhes de verificação como números de telefones, documentos, endereço, e-mail, e assim por diante. A ganância resultante de ideia de ganhar um prêmio leva o usuário a entregar todo tipo de informação, o que é usado para vitimá-lo futuramente. (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

2.6 E-MAIL

O e-mail é usado em uma variedade de fraudes, mais abordaremos apenas três com base nos estudos de BASTA, Afred; BASTA, Nadine; BROWN, Mary (2014)

- Um engenheiro social pode enviar um e-mail de uma conta que aparenta ser de uma conta legitima de TI, como do administrador de redes, por exemplo, entretanto, o endereço de retorno é do próprio engenheiro e neste mesmo e-mail apresenta problemas, alegando que a solução é o usuário enviar a sua senha para ajudar a corrigi-los. Mas, um administrador legitimo nunca pede senhas para resolução de problemas de *login*, porém, esse tipo de fraude costuma ser bem-sucedida;

- O outro truque é enviar e-mail para participar de competições para assim receber prêmios. Neste caso o engenheiro anexa um formulário para preenchimento com dados pessoais, como nomes completos, telefone, rg, cpf, entre outros, que nos quais muitas das

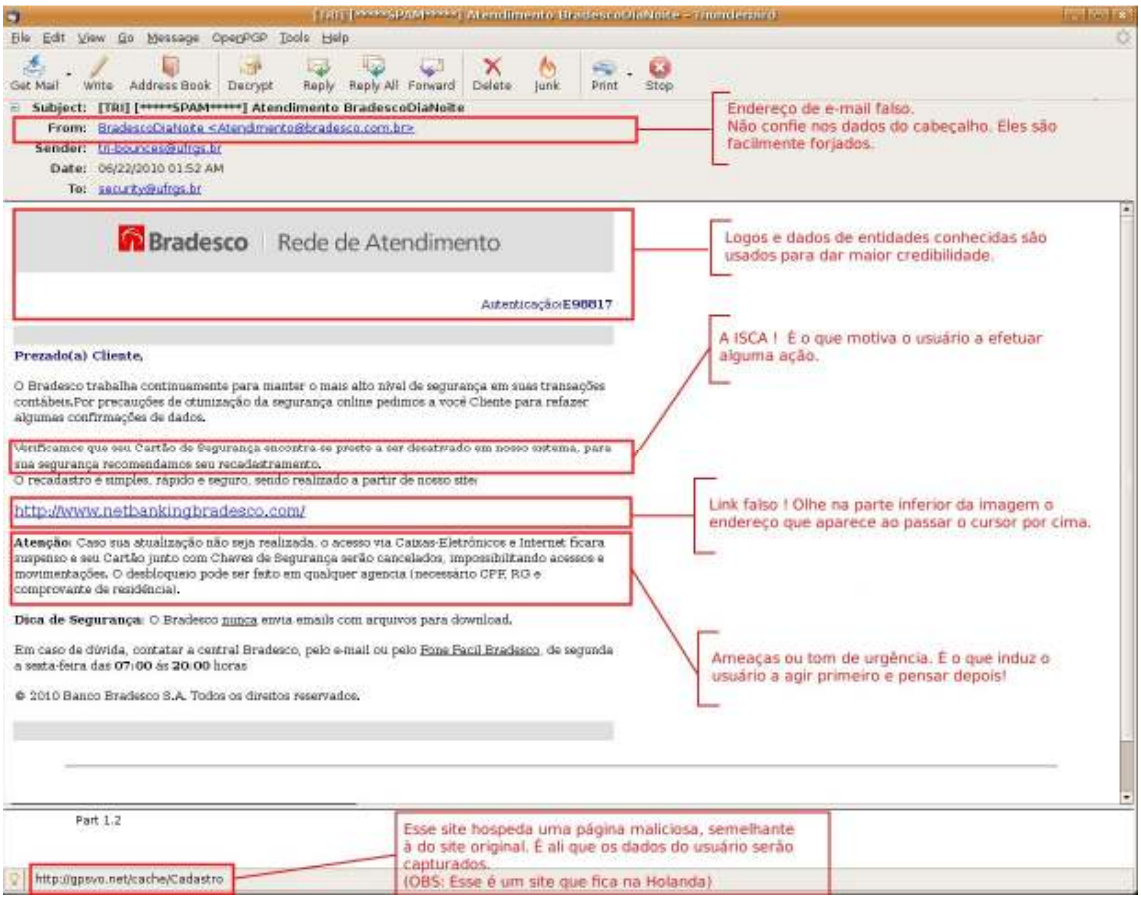
vítimas usam em outras contas online; assim, ao fornecer esses dados colocam em riscos todas as contas com combinações de nome de usuário e senhas. E os usuários caem neste golpe, com o desejo de ganhar prêmios ou dinheiro.

- Por último o esquema final é chamado de *phishing* que segundo a Central de Segurança e Proteção da Microsoft nada mais é que:

> "Um tipo de roubo de identidade online. Ele usa e-mail e websites fraudulentos que são concebidos para roubar seus dados ou informações pessoais, como números de cartão de crédito, senhas, dados de contas ou outras informações. Os golpistas podem enviar milhões de mensagens de e-mail fraudulentas com links para sites fraudulentos que parecem vir de sites confiáveis, como seu banco ou administradora de cartão de crédito, e solicitar que você forneça informações pessoais. Os criminosos podem usar essas informações para diversos tipos de fraude, como roubar o dinheiro de sua conta, abrir novas contas em seu nome ou obter documentos oficiais usando sua identidade. "

A Figura 2 nos mostra um exemplo de e-mail fraudulento evidenciando características que comprovam a sua natureza.

Figura 2 - Anatomia de uma mensagem falsa.



Fonte: (UFRGS)

2.7 MENSAGEM INSTANTÂNEA

Neste caso o engenheiro social tenta ficar amigo da vítima para obter informações e apresentar-lhe um link de web que possa querer visitar. Normalmente contendo pornografia. Porem estas mensagens são postadas em redes sociais (Orkut, Twitter, Facebook) ou enviadas via software de mensagem instantânea (MSN, ICQ, Yahoo Messenger) que contém mensagens de propaganda ou se passa por alguma empresa conhecida, solicitando acessos através de links, que na verdade contém algum vírus ou instala programas maliciosos para captura de informações do computador ou para permissão de acesso de algum invasor. (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

A Figura 3 mostra o uso de *phishing* através do serviço de mensagens do facebook. Neste caso, o engenheiro social envia uma mensagem dizendo que aconta

será desativada imediatamente porque alguém tem relatado as ações da vitima sendo que, talvez, ela tenha escrito algo abusivo ou fez upload de uma imagem que poderia ser ofensiva ou nociva a outros usuários. Pedindo a confirmação da sua conta, para interromper o aviso desativação da conta. E, em anexo envia um link que direciona para um página identica a de login do facebook solicitando email e senha de autenticação mais essas informações caem no email do engenheiro.

Figura 3 - Facebook usado para ataques de phishing.

Fonte: (Websense Security Labs, 2010)

2.8 COMUNICAÇÃO POR TELEFONE

Engenheiros sociais têm um leque de ferramentas com as quais podem explorar a comunicação telefônica com finalidade maliciosa. Eles podem alterar sons de fundos, suas próprias vozes como, por exemplo, alterar uma voz grasso masculina com sotaque por uma voz delicada e feminina. Engenheiros sociais também têm

ferramentas gerando falsas entradas na tecnologia de identificação fazendo parecer uma ligação verdadeira e legitima.

Atendentes de *help desk* são alvos vulneráveis porque recebem mais acesso a informação que um funcionário normal e eles, em geral, trabalhão sob pressão para responder bem o máximo de chamadas que conseguirem.

Ao ligar para um funcionário especifico, pode ser mais eficiente ligar para outro funcionário e pedir para ele transferir a ligação. Isso faz quem liga pareça mais confiável do que se tivesse ligado direto para a vítima.

Hackers com muita frequência se passam por técnicos que contatam usuários alvos para informá-los, por exemplo, que pode ter tido uma cobrança, excessiva em suas contas de telefone e depois de convencer a vítima dessa premissa, pede mais informações pessoais. (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

2.9 MERGULHO NO LIXO

Mergulho no lixo (*dumpster diving* em inglês) ato o efeito de revirar o lixo de uma empresa em geral é uma grande fonte de informações importantes, assim como de hardware e software. E é no lixo que pode esconder informações sensíveis. As pessoas jogam de tudo no lixo, inclusive extrato bancário, informações de cartões de créditos, papel rabiscado com telefones, senhas de acesso aos diversos sistemas, sejam eles de uma conta de e-mail ou senhas bancárias etc.; (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

2.9.1 A importância do descarte apropriado do lixo

A política de segurança de uma organização deve especificar cuidadosamente qual é informação é crítica qual não é, e então determinar como tratar do lixo. Alguns documentos podem não ser considerados críticos, como caderneta de funcionários e declarações políticas da empresa. Entretanto, isso muitas vezes pode dizer aos hackers que tipo de segurança física e de rede esperar quando tentarem invadir. (BASTA, Afred; BASTA, Nadine; BROWN, Mary 2014)

A política de segurança é umas das maneiras mais eficientes no combate a engenharia social e será apresentada e detalhada no capítulo seguinte deste trabalho.

3. POLÍTICA DE SEGURANÇA E SUAS NORMAS.

A Política de Segurança é um estatuto que define o que é considerado pela Empresa como aceitável ou inaceitável, contendo ainda referências às medidas a serem impostas aos infratores. Para evitar ou diminuir o risco de informações confidenciais serem acessadas indevidamente, perdidas ou até mesmo alteradas, é necessário que haja uma série de procedimentos estabelecidos para que essas informações venham transitar na empresa. (SCHWARTAU, 2010).

Segundo Schwartau (2010), a política de segurança da informação pode ser definida como uma série de instruções claras com a finalidade de fornecer orientação para o usuário. Esse é um elemento de suma importância para o controle da segurança da informação para combater e prevenir possíveis ameaças ou ataques que venha a comprometer as informações. A seguir serão apresentadas as políticas de segurança que incluem questões de prevenção. Um ótimo exemplo são as políticas relacionadas à abertura de e-mails, que podem ocasionar a instalação de vírus, Cavalos de Troia e etc., ou em empresas que possuem e-mails corporativos e criam suas próprias políticas.

- Quais ameaças ou que tipo de ameaça pode atingir a empresa.
- Quais prejuízos à empresa teriam se uma dessas situações ocorrer.

Ao elaborar uma política de segurança, Alves (2010) informa que se deve levar em consideração que existem funcionários que não têm entendimento da linguagem técnica. Portando, devem-se criar documentos de fácil entendido para os funcionários. O documento também deve deixar bem claro a importância da política de segurança para que os funcionários não encarem isso como algo desnecessário. Devem ser criados dois documentos separadamente, onde um deles apresentará as políticas e o outro abordará os procedimentos. É importante ressaltar também que a política de segurança nunca deve ser imutável ou inflexível, pois as novas técnicas de ataques usando a engenharia social estão surgindo a cada dia assim como as próprias tecnologias para combatê-las. Para que a política de segurança esteja sempre atualizada, devem-se estabelecer reestruturações regulares com o objetivo de

identificar as novas ameaças e assim combatê-las através das tecnologias e ou procedimentos adequados.

3.1 OBJETIVO DA POLÍTICA DE SEGURANÇA

A política tem como objetivo proteção do conhecimento e da infraestrutura, com o objetivo de atender os requisitos legais, viabilizar os serviços prestados e evitar e/ou reduzir os riscos possíveis ameaças. Orientação e o estabelecimento de diretrizes para a proteção das informações, prevenção de ameaças e a conscientização da responsabilidade dos funcionários. É conveniente que a gestão da segurança da informação esteja alinhada e em conjunto com os outros processos de gestão. (FIPECAFI, 2011).

3.2 NORMAS DE SEGURANÇA

As Normas de Segurança segundo Silva (2003) são os mecanismos formais que definem os objetivos da organização em termos de segurança, ou seja, documentos compostos por todas as regras, concretizando em detalhe as linhas orientadoras estabelecidas na Política de Segurança. É neste documento que deverão estar referenciadas as tecnologias utilizas na Empresa e a forma segura de utilizá-las.

3.3 OS GRUPOS DE INTERESSE NA ELABORAÇÃO DA POLÍTICA DE SEGURANÇA

De acordo Silva (2003) para uma política de segurança se torne apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de empregados dentro da organização. É singularmente importante que a gerência corporativa suporte de maneira completa o processo da política de segurança, caso contrário haverá pouca chance que ela atinja o objetivo desejado. Abaixo descreve os indivíduos que deveria estar envolvida na criação e revisão dos documentos da política de segurança:

- O administrador de segurança do site;
- A equipe técnica de TI;

- Os Administradores de grandes grupos de usuários dentro da organização;
- A equipe de reação a incidentes de segurança;
- Os Representantes de grupos de usuários afetados pela política de segurança;
- O Conselho Legal;

A ideia é trazer representações dos membros, gerentes responsáveis sobre o orçamento e política, pessoal técnico que saiba o que pode e o que não pode ser suportado, e o conselho legal que conheça as decorrências legais das várias políticas. Em algumas organizações, pode ser apropriado incluir pessoal de auditoria.

3.4 A IMPORTÂNCIA DE DOCUMENTAR A POLÍTICA DE SEGURANÇA

Silva (2003), informa que nunca é demais acentuar a importância de um corpo documental coeso, atual e apropriado. Ao criar uma política de segurança clara e objetiva, a Empresa deve evidenciar os seus objetivos, sem margem para dúvidas. A documentação deverá servir de orientação e referência para todos os colaboradores da organização, no que concerne à segurança.

3.5 CRITÉRIOS PARA DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA

De acordo com o TCU (2012) a divulgação dever ser ampla a todos os usuários internos e externos à instituição. E é um passo indispensável para que o processo de implantação da política tenha sucesso. Ela deve ser de conhecimento de todos que interagem com a instituição e que, direta ou indiretamente, serão afetados por ela. É de extrema importância que fique bem claro, para todos, as consequências advindas do uso inadequado dos sistemas computacionais e de informações, as medidas preventivas e corretivas que estão a seu cargo para o bom, regular e efetivo controle dos ativos computacionais. A política fornece orientação básica aos agentes envolvidos de como agir corretamente para atender às regras nela estabelecidas. É importante, ainda, que a ela esteja permanentemente acessível a todos.

Mais caso ela seja violada a própria Política de Segurança de Informações deve prever os procedimentos a serem adotados para cada caso de violação, de

acordo com a severidade, a amplitude e o tipo de infrator que a perpetra. A punição pode ser desde uma simples advertência verbal ou escrita até uma ação judicial.

3.6 REGRAS BÁSICAS DE PROTEÇÃO E BOM FUNCIONAMENTO DA POLITICA

Alves (2010) afirma que a política de segurança deve conter algumas regras primordiais para um bom funcionamento da segurança como:

- Os empregados devem assumir uma postura proativa em relação à proteção das informações e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação;
- As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;
- Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
- Somente softwares homologados podem ser utilizados no ambiente computacional da empresa;
- Todo usuário, para poder acessar dados das redes de computadores utilizadas, mas deverá possuir um código de acesso atrelado à uma senha previamente cadastrada, sendo este pessoal e intransferível, ficando vedada a utilização de códigos de acesso genéricos ou comunitários;
- Não é permitido o compartilhamento de pastas nos computadores de empregados da empresa. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

3.7 MANTENDO A POLÍTICA SEMPRE FLEXÍVEL

A política não só pode ser alterada, como deve passar por processo de revisão definido e periódico que garanta a reavaliação a qualquer mudança que venha afetar a análise de risco original, tais como: incidente de segurança significativo, novas vulnerabilidades, mudanças organizacionais ou na infraestrutura tecnológica. Além disso, deve haver análise periódica da efetividade da política, demonstrada pelo tipo,

volume e impacto dos incidentes de segurança registrados. É desejável, também, que sejam avaliados o custo e o impacto dos controles na eficiência do negócio, a fim de que esta não seja comprometida pelo excesso ou escassez de controles. É importante frisar, ainda, que a política de segurança deve ter um gestor responsável por sua manutenção e análise crítica. (TCU, 2012).

3.8 TREINAMENTO E CONSCIENTIZAÇÃO

Um dos assuntos mais entediantes para a grande maioria dos funcionários é sobre a política de segurança da informação. Por isso é essencial que haja bons artifícios cativá-los e inclusive entusiasmá-los a aplicá-los. Uma empresa que realmente leva a questão da segurança da informação a sério, passa a treinar seus funcionários assim que são admitidos, de maneira que nenhum funcionário possa receber acesso a um microcomputador antes de participar de pelo menos uma aula básica sobre conscientização. Um ótimo aspecto a ser abordado que pode funcionar como um grande agente motivador para os funcionários é esclarecê-los de que a segurança da informação não é um assunto de interesse somente da empresa, mas também dos próprios, pois a empresa possui informações particulares a respeito dos mesmos. Os funcionários perceberão que ao colaborarem estarão protegendo não somente informações da empresa, mas também suas informações pessoais (FONSECA, 2009).

Às vezes, o treinamento deve ser adaptado de acordo com os requisitos específicos de cada grupo dentro da organização, só existe uma maneira de manter seguros os planos da empresa: ter uma força de trabalho treinada e consciente, pois apesar de muitas vezes as políticas serem aplicadas a todos os funcionários, há situações em que serão necessárias políticas específicas para determinados cargos ou grupos, como por exemplo, os gestores, pessoal da tecnologia, usuários de microcomputadores entre outros. É fundamental em um programa de conscientização deixar bem claro a importância de seguir as políticas de segurança corretamente e os danos que a empresa possa sofrer se estas não forem seguidas. Os funcionários também devem ser advertidos a respeito das consequências se não cumprirem as normas e procedimentos estabelecidos, pois muitas vezes, os próprios funcionários ignoram ou até mesmo negligenciam os procedimentos que acham desnecessários,

ou aqueles considerados tediosos. Elaborar um resumo dessas consequências e divulgá-los é um ótimo procedimento a ser realizado. Algo muito interessante que também pode ser colocado em prática é a recompensa para os funcionários que seguem as boas práticas de segurança. Pois o incentivo é sempre algo muito motivador. A questão da prevenção nas empresas não é uma tarefa fácil, porque a muitas das empresas não dá à mínima, elas concentram seus recursos financeiros somente na manutenção de sistemas e em novas tecnologias, ao invés de destinar parte desses recursos para treinamento e conscientização dos funcionários. Recursos como *Intranet* ou correio eletrônico podem ser tão úteis para a divulgação, por exemplo, lembretes de segurança como mudança de senhas (FONSECA, 2009).

Um bom e objetivo processo de conscientização sobre segurança da informação não pode deixar de lado os seguintes itens:

- Táticas empregadas pelos engenheiros sociais para invadirem as informações.
- Como identificar a ação de um engenheiro social.
- Como agir ao desconfiar.
- A quem reportar as tentativas de ataque.
- Não confiar em pessoas que fazem solicitações de informações, sem que elas sejam de confiança.
- Como proteger suas informações.
- A obrigação do cumprimento das políticas de segurança.
- Eliminação de documentos que contenham informações confidenciais.
- Deixar bem claro que testes serão feitos periodicamente dentro da organização para verificar quais funcionários estão procedendo corretamente.
- Fornecer material informativo como, por exemplo, lembretes através do meio de comunicação.
- Parabenizar publicamente os funcionários que cumprem as regras.

Testes de vulnerabilidades usando a engenharia social podem ser feitos periodicamente com o objetivo de encontrar falhas ou descobrir o descumprimento das políticas de segurança e até mesmo pontos fracos no próprio treinamento dos mesmos. Tudo isso se resume em uma reeducação na organização de maneira a inserir uma nova cultura que abrange cem por cento da empresa, pois qualquer falha poderá ser fatal (FONSECA, 2009).

3.9 PLANO DE RESPOSTAS A INCIDENTES

Segundo Absoluta (2002), não existe infraestrutura de segurança que venha garantir cem por cento de proteção, pois as falhas sempre existirão, por mais remotas que sejam. Segundo a Microsoft (2010), coloca que, ter um plano facilmente acessível ajudará a garantir que os procedimentos corretos sejam seguidos em caso de um incidente. Portanto as empresas devem estar preparadas para reconhecer, analisar e responder aos incidentes de segurança o mais rápido possível, pois isso é fator fundamental para amenizar os estragos ou diminuir custos com reparos. É importante que as experiências anteriores com outros incidentes sejam usadas para prevenir ocorrências semelhantes no futuro ou até mesmo para aprimorar a segurança atual. O documento que define as diretrizes para tratar incidentes de segurança chama-se Plano de Resposta a Incidentes. Ele possui os procedimentos e medidas a serem tomadas para remediar, corrigir ou contornar os incidentes. Como já foi abordado anteriormente, cada empresa possui suas particularidades e culturas organizacionais, portanto, os procedimentos de respostas para os incidentes são muito particulares, pois variam de organização para organização. O mais importante é que independente do porte da empresa ou do seu ramo de atividades, ela deverá possuir o seu próprio Plano de Respostas.

As seguintes medidas não podem ser deixadas de lado em um Plano de Resposta a Incidentes:

- Identificar a autoria dos ataques, assim como sua seriedade, estragos causados e responsáveis pelo incidente.
- Divulgar o mais rápido possível o acontecimento ocorrido para que o mesmo incidente não ocorra em outras áreas da empresa.
- Tomar as medidas necessárias para restaurar aquilo que foi afetado como, por exemplo, mudar senhas, trocar funcionários, aumentar o nível de controle.
- Contatar os órgãos de segurança para que o fato seja registrado, assim como tentar entrar em contado com os responsáveis pelos ataques.

Os tópicos citados a cima são extremamente importantes para a criação de uma política de segurança da informação que procura se proteger, não devendo ser

considerada como uma lista completa de procedimentos ou até mesmo porque isso varia de acordo com o planejamento de cada empresa.

4. ANÁLISE DE UMA POLÍTICA DE SEGURANÇA DE UMA EMPRESA

Atualmente a maiorias das empresas prezam pela segurança, confiabilidade e integridade de todos os dados em todos os setores. E a partir das devidas funções desempenhadas, delimitam acessos restritos e controlados através de sistemas e regras, além de controle de vírus, acesso a sites, regras de spam para e-mails, bloqueios de portas para acesso a dispositivos móveis e controle de acesso a usuários nos softwares utilizados pela empresa.

Segundo Silva (2003):

> "O responsável pela implementação da segurança dos sistemas de informação na Empresa tem, como primeira missão, e mais importante, a garantia da segurança da informação que protege. Esta garantia é conseguida mediante a utilização de vários instrumentos, que deverão abranger as diversas áreas".

Mesmo com todas essas regras e políticas, pessoas mal-intencionadas, como os engenheiros sociais conseguem retirar, apagar informações vitais de dentro das empresas.

O próximo tópico irá abordar a pesquisa feita com o supervisor de suporte técnico de uma empresa de grande porte, e de como a reformulação de uma política de segurança pode educar deixando os objetivos dela mais claros e ajudar os usuários a combater esses ataques de forma efetiva, a fim de proteger todas as suas informações.

4.1 NA EMPRESA

Uma empresa no ramo hospitalar possui aproximadamente 2100 funcionários sem considerar os médicos e terceirizados, os quais trabalham com um grande número de acesso a informações como cadastros de pessoas, consultas, doenças, cirurgias, exames, e muitos outros que são alimentados em sistemas ERP's todos se reportam a uma única base de dados, abrangendo todos os setores, trazendo informações em tempo real dos pacientes.

De acordo com o supervisor de suporte técnico que trabalha a 11 anos na empresa funciona desta maneira, todos os pacientes que irão fazer seu primeiro

atendimento, seja ele uma simples consulta agendada, ou um atendimento de urgência, são cadastrados no sistema e recebem um número de identificação, para fácil controle nos demais setores. O próximo a atendê-lo é um médico que irá examiná-lo e inserir o diagnóstico no sistema, e se por ventura for necessário, exames, medicamentos até mesmo cirurgias, procedimentos pós-operatório tudo será colocado também no sistema.

A empresa possui uma política de segurança aparentemente branda levando em consideração a responsabilidades atribuída aos usuários, porque à responsabilidade maior fica por parte da própria TI, que através da sua infraestrutura, procura “fechar as portas”, bloqueando os computadores para que não se faça o uso de pen drives, HD externos, celulares conectados ao computador, drives de CD/DVD ou qualquer outro dispositivo de armazenamento de informação, e também, broqueio a instalação ou desinstalação de software. O uso dos programas, somente homologados pelo setor de TI sendo todos originais e atualizados. Tendo em suas rotinas diárias, backup dos dados em dispositivos como fitas de backup e em servidores localizados em locais diferentes. A rede, e assegurada tendo ela sobre domínio, firewalls, servidores de autenticação de usuário, de proxy e acesso controlado à internet e e-mail, liberando somente a quem e realmente é necessário o uso, e mediante a autorização da diretoria e aceitação dos termos da política de segurança.

O acesso à os usuários e criado no servidor de autenticação onde eles são organizados em grupos, onde cada setor representa um grupo e cada novo usuário e locado no grupo do seu respectivo setor. Assim o novo usuário passa a ter acesso tanto no sistema quanto à os diretórios da rede somente do seu setor.

Os recursos de redes, servidores e banco de dados são todos monitorados por com controle de temperatura de salas de servidores, controle de disponibilidades dos recursos de redes e controle da conformidade do banco de dados e sistemas da utilizados no hospital.

Um treinamento muito simples e com uma linguagem técnica dificultava a compreensão e a educação sobre a importância da segurança a informação aos funcionários iniciantes, que muitas vezes não entendem muito de informática, e essa método de apresentar a política fazia que os usuários tratassem ela como algo

burocrático e sem importância não tomando os devidos cuidados, facilitando assim, um ataque de um engenheiro social.

Todas essas informações são monitoradas, controladas, para que possam combater todos os ataques que possam ser deferidos por engenheiros sociais, vírus, malware entre outros que possam lesar ou roubar essas informações. Mas faz se necessário uma política e um treinamento apropriado afim de educar os funcionários sobre a importância de informação e como mantê-la segura para evitar possíveis ataques, começando pela apresentação da política de segurança mais didática, bem estruturada e flexível, desenvolvida para cada setor e função, passando por um treinamento aos funcionários a fim de conscientizar os mesmos dos riscos, como diz sobre o assunto Silva (2003), estes são os mecanismos formais que definem os objetivos da organização em termos de segurança. E por fim manter junto à área de tecnologia da informação um plano de resposta a qualquer tipo de ataque, para que assim a segurança possa estar completa.

4.2 CRIANDO UMA POLÍTICA E ESCLARECENDO SEU OBJETIVO

Segundo o supervisor de suporte técnico, antes de qualquer treinamento, controle ou ajuste na empresa foi criado, uma nova política de segurança, desenvolvida por um conjunto multidisciplinar envolvendo vários setores e vários profissionais, sendo administrativos, financeiros, auditorias, médicos, enfermeiros entre e outros que possam tenha acesso e possam comprometer a segurança de alguma forma.

Vale salientar que sucesso disto está diretamente relacionado ao envolvimento e à atuação da alta administração. Quanto maior for o comprometimento da administração superior com os processos de elaboração e implantação de uma nova política, maior a probabilidade de ela ser efetiva e eficaz.

Essa política continha regras claras que possam inibir os quaisquer ataques seja de engenheiros sociais, vírus entre outros, demonstrando em poucas palavras o que não pode ser acessado, e se acessado como inibir qualquer ataque.

Essa política deve ser flexível e coerente. Dentro dela deve conter além das normas, regras e controles existentes as punições cabíveis para qualquer violação por parte do usuário.

Após a criação da nova política de segurança, é essencial que ela seja divulgada e esteja permanentemente acessível a todos, para que todos os funcionários fiquem conscientes das novas normas a fim de alterar o pensamento e a forma de trabalho antigo.

4.3 APLICAÇÃO

A partir do primeiro momento que o novo funcionário integrar o corpo de funcionários ele deve receber um treinamento, e se possível, tirar o primeiro dia, todo para isso, para que sejam demonstradas as formas, políticas e condutas de trabalho a fim de conscientizar, educando ao máximo o novo membro. E para os funcionários que tem um tempo de casa, o treinamento é feito em horários alternativos para não atrapalhar o andamento do setor, quando não, o próprio encarregado ou chefe de setor é treinado para demonstrar a mudanças da nova política e importância de segurança da informação.

4.4 PRIMEIRO TREINAMENTO

Segundo Silva (2003) “Técnicas sobre segurança deverão ser ações em que se instruam os utilizadores sobre como realizar as tarefas cotidianas que lhes competem, de modo a não afetar a segurança dos sistemas”.

Seguindo assim a orientação de Mitnick (2003):

> “A orientação básica que deve ser lembrada durante o desenvolvimento de um programa de treinamento e conscientização em segurança é que o programa precisa se concentrar em criar em todos os empregados a consciência de que a sua empresa pode ser atacada a qualquer momento. Eles devem aprender que cada empregado tem um papel na defesa contra qualquer tentativa de entrar nos sistemas de computadores ou de roubar dados confidenciais”.

De acordo com esta orientação, quando o funcionário é contratado ele recebe um treinamento de orientação da política de segurança da informação ministrado por um dos profissionais da área de Tecnologia da Informação.

Nesse momento é o momento ideal de treinar o usuário por isso o profissional de tecnologia da informação TI responsável é muito importante, porque é ele que vai explicar o que é permitido para utilização da informação, como trabalhar com os e-mails corporativos, com o sistema implantado na empresa e esclarecer e justiçar a política de segurança e o mais importante, maneiras de neutralizar uma possível ação tanto de vírus como dos engenheiros sociais.

De acordo com o supervisor de suporte técnico o treinamento para identificação de possíveis ameaças, e partem dos princípios abaixo as formas de combate que são apresentados neste primeiro treinamento:

- Os empregados devem estar em alerta contra roubos e fraudes de informações porque acontecem com muita frequência.
- As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções e conhecimento da área de TI;
- Senhas, chaves e outros recursos de caráter pessoal são intransferíveis e de responsabilidade do usuário;
- Somente softwares instalados pela tecnologia da informação podem ser utilizados;
- Todo usuário, para poder acessar dados das redes de computadores devem possuir um código de acesso atrelado a uma senha previamente cadastrada;

O primeiro treinamento e feito de forma clara, didática e objetiva, além de criar a ideia da importância e de como defender as informações, consolidam ainda mais a proteção dos dados.

4.5 APRESENTAÇÃO DA POLITICA

Após o treinamento, supervisor de suporte técnico relata que por fim, vem à apresentação da política de segurança, que através de um ofício que consta todas as normas, regras e condutas, consolidam tudo aquilo apresentado anteriormente, e

fortalece ainda mais a ideia de que a segurança dos dados alimentados é de extrema importância que em hipótese alguma pode ser roubada.

4.6 A PRÁTICA

Com o primeiro treinamento concluído e a apresentação da política feita, é necessário demonstrar na prática como acontece um ataque de um engenheiro social, vírus, *malware* e outros tantos que possam representar um perigo eminente a informação.

Como relata o supervisor de suporte técnico, deve-se demonstrar como um engenheiro social costuma atacar, começando por uma simples conversa para retirar informações até a um e-mail estranho que possa representar um ataque ou um vírus.

Já com uma ideia de como identificar um ataque, com a política em mente, e sabendo como pode ser um ataque, fica mais fácil para o usuário até então leigo criar formas de detê-los e defendendo assim informação.

Desta forma, o funcionário fica esclarecido sobre métodos de defesa e conduta dentro da empresa, a fim de dar continuidade à política de segurança.

5. CONSIDERAÇÕES FINAIS

Nesta avaliação realizada, percebe-se que após alguns meses de aplicação do novo modelo da política de segurança, o controle e treinamento dos funcionários a evolução foi extremamente satisfatória, de acordo com o administrador de banco de dados e, responsável pelo suporte técnico houve, também, um interesse e uma motivação por parte dos usuários em relação à segurança da informação, que em razão da nova política de segurança da informação, aproveitaram para dar palestras e treinamentos internos para outros funcionários. Explicando, não somente, a importância de assegurar a informação mais também, mantê-la mais sigilosa possível, para não comprometer e/ou constranger os pacientes, mantendo assim, a ética do profissional de saúde.

Assim como proposto a mudança atingiu seus objetivos criando uma barreira mais eficiente contra os ataques, já que os funcionários entenderam o valor e significado e se conscientizaram da importância da segurança das informações, assim, como declarou Mitnick (2003) que só existe uma maneira de manter seguros os seus planos: ter uma força de trabalho treinada e consciente.

6. CONCLUSÃO

A presente monografia foi feita a partir de revisões bibliográficas e aplicação de questionário que abordou a utilização da política de segurança na empresa, focando no conceito da criação de uma política reformulada, didática, clara e objetiva para educar os funcionários sobre a importância da segurança da informação e como combater a engenharia social.

Ao término deste trabalho, podemos afirmar que atingimos o objetivo no que se diz respeito ao aprofundamento do conhecimento sobre o tema e aplicação de uma política de segurança muito bem implementada, de maneira que, se tornou compreensível a maioria dos funcionários, que assimilaram a importância de assegurar a informação em suas diversas naturezas para um combate mais eficaz a engenharia social.

REFERÊNCIAS BIBLIOGRÁFICAS

ABSOLUTA. **Resposta a Incidentes de Segurança - (PARTE 1). 2002**. Disponível em: <http://www.absoluta.org/seguranca/seg_resposta_incidente_1.htm>. Acesso em: 30 de novembro de 2015.

ADACHI, Tomi. **Gestão de Segurança em Internet Banking**. São Paulo: FGV, 2004. 121p. Mestrado. Fundação Getúlio Vargas – Administração. Orientador: Eduardo Henrique Diniz.

Artigo Cássio Bastos Alves, 2010, **Engenharia social**. Disponível em <http://monografias.brasilescola.com/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm>. Acessado no dia 26 de novembro de 2015.

Artigo FIPECAFI, **TI V1.0 Jan/2011**. Disponível em <http://www.fipecafi.org/downloads/ti/psi-politica-seguranca-informacao-fipecafi-ti-v1-01.pdf>. Acessado em 26 de novembro 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. NBR ISO/IEC 17799: 2005** tecnologia da informação: técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. NBR ISO/IEC 27002:2013.**

BASTA, Afred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. Tradução Lizandra Magon de Almeida. São Paulo: Cengace Learning.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações.** São Paulo: Editora SENAC São Paulo, 1999

FONSECA, Paula F. **Gestão de Segurança da Informação**: O Fator Humano. 2009. Redes e Segurança de Computadores, Universidade Católica do Paraná, Curitiba, 2009.

MENDES DA SILVA FILHO; ANTONIO. **Segurança da Informação: Sobre a Necessidade de Proteção de Sistemas de Informações**. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm>. Acesso em: 14 setembro 2015.

MICROSOFT, **Respondendo a incidente de segurança de TI**. <http://technet.microsoft.com/pt-br/library/cc700825.aspx>. Disponível em 30 de novembro de 2015.

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

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

Phishing Central de Segurança e Proteção da Microsoft Perguntas frequentes: Disponível em: <https://www.microsoft.com/pt-br/security/online-privacy/phishing-faq.aspx>. Acessado em: 25 de novembro 2015.

PILARES da segurança da Informação: Disponível em: <http://www.f4.inf.br/seguranca-da-informacao/>. Acesso em: 14 setembro 2015.

SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digital.** Rio de Janeiro: Campus, 2001.

SCHNEIER, BRUNCE. **Segredos e mentiras sobre a proteção na vida digital.** Rio de Janeiro: Corpus LTDA 2001.

SCHWARTAU, Winn. **Engenharia social**: pessoas ainda são elo mais fraco. [S.l.:s.n.], 2010. Disponível em. Acesso em: 22 de fevereiro de 2013.

SÊMOLA, M. 2003: **Gestão da Segurança da Informação**. 1.Ed. Rio de Janeiro: Campus, 2003.

STAIR, Ralph M.; REYONLDS George W..**Princípios de Sistemas de Informação.** Trilha 2015.

Tribunal de Contas da União (TCU). **Boas Práticas em Segurança da Informação.** Brasília: Secretaria de Fiscalização de Tecnologia da Informação, 2012.

Universidade Federal do Rio Grande do Sul. **Anatomia de uma mensagem falsa**: Disponível em:<http://www.ufrgs.br/tri/Documentos/image.jpeg>. Acessado em: 02 de dezembro de 2015.

Websense Security Labs. **Facebook used for phishing attacks and open redirects**: Disponível em: <http://community.websense.com/blogs/securitylabs/archive/2010/11/29/facebook-used-for-phishing-attacks-and-open-redirects.aspx>. Acessado em: 02 de dezembro de 2015.

ANEXOS E APÊNDICES

Qual é seu Cargo/função?

Há quanto tempo trabalha na empresa tempo de empresa?

Como a empresa funciona?

A empresa possui uma política para proteção das informações?

Sendo a política branda como ela então assegura a informação?

Qual é a maneira que a empresa utiliza hoje para apresentar o ambiente informático e as políticas de segurança a os usuários?

Qual é o objetivo de uma reestruturação da política de segurança?

Porque se faz necessário um conjunto multidisciplinar para elaboração de uma política de segurança?

Depois de reformulada a política como ela e apresentada para os funcionários?

E como foi feita o treinamento e prestação da nova política.

E depois de toda essa mudança na política e forma de apresenta lá quais foram os resultados?

Como e feito o controle dos usuários acessos e de uma maneira geral, todo o parque tecnológico?