CENTRO PAULA SOUZA

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

ENGENHARIA SOCIAL: FRAUDE EM CERTIFICAÇÃO DIGITAL

JULIANA RODRIGUES DA SILVA

Americana, SP
2015

CENTRO PAULA SOUZA

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

ENGENHARIA SOCIAL: FRAUDE EM CERTIFICAÇÃO DIGITAL

JULIANA RODRIGUES DA SILVA

Juli.rs@outlook.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 Prof. Dra. Acácia Ventura.

Área: Engenharia social

Americana, SP
2015

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

Silva, Juliana Rodrigues da
S58e Engenharia social: fraude em certificação digital. / Juliana Rodrigues da Silva. – Americana: 2015.
54f.

Monografia (Graduação em Tecnologia de Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Dr. Acácia de Fátima Ventura

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

CDU: 681.518.5

JULIANA RODRIGUES DA SILVA

ENGENHARIA SOCIAL: FRAUDE EM CERTIFICAÇÃO DIGITAL

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: Engenharia Social

Americana, 23 de junho de 2015.

Banca Examinadora:

Acácia de Fátima Ventura (Presidente)
Doutora
Fatec Americana

Diógenes de Oliveira (Membro)
Mestre
Fatec Americana

Benedito Aparecido Cruz (Membro)
Especialista
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer a minha orientadora Doutora Acácia Ventura que me apoiou com empenho e dedicação no desenvolvimento de minha pesquisa científica.

A todos os professores da Instituição de Ensino Fatec Americana, em especial aos professores do curso de Segurança da Informação, que me auxiliaram em meu desenvolvimento profissional, sempre acreditando no meu potencial.

Aos meus colegas de turma, com os quais convivi em plena harmonia, agradeço pela amizade, paciência e pela troca de experiências profissionais, em especial a minha irmã Jaqueline que também foi minha colega de estudos.

Ao meu irmão Jorge Henrique por ter me apresentado a Fatec Americana e apoiar meus estudos. Aos meus pais, por sempre estarem presentes.

À Secretaria de Graduação da FATEC - Americana, pelo apoio, e principalmente, pela amizade demonstrada pela Coordenadora de curso Cristina Aranda.

DEDICATÓRIA

À Minha Família, em especial aos meus pais e irmãos que me ajudaram nessa conquista.

RESUMO

Com o avanço da tecnologia e a necessidade de autenticar-se no meio digital de forma segura surgiram os certificados digitais, porém, desde tempos remotos o homem explora as vulnerabilidades existentes em todos os ambitos com o intuito de obter vantagens financeiras. Diante de tais fatos um meio tão amplo de autenticação no mundo digital despertou o interesse dos famosos engenheiros sociais, que se utiliza de técnicas específicas para obter informações relevantes em prejuízo de terceiros. O Governo Federal brasileiro implementou uma hierarquia vinculada a infra estrutura de Chaves Públicas denominada ICP Brasil, com o objetivo de tornar as emissões de certificados digitais mais seguras, porém, essa hierarquia sofre, diariamente, com as tentativas de fraudes executas pelos engenheiros sociais. Nessa pesquisa objetiva-se entender as técnicas utilizadas pelos engenheiros sociais quando da emissão de certificados digitais, utilizando como metodologia científica o método hipotético dedutivo, sendo a pesquisa classificada como pesquisa básica, qualitativa, descritiva, bibliográfica e documental. O mundo evoluiu e se tornou digital, sendo necessário proteger o maior ativo que uma organização possui: a informação. Porém, apesar dos procedimentos de segurança implementados, os engenheiros sociais sempre procuram por brechas nos sistemas para alcançarem o seu propósito. Portanto, para tornar as políticas de segurança eficientes, elas devem estar em constante evolução, acompanhando a evolução humana.

Palavras Chave: Segurança da Informação; Certificado Digital; Engenharia Social.

ABSTRACT

With the advancement of technology and the need to authenticate the digital environment securely, digital certificates were born, however, since ancient times man exploits the vulnerabilities in all areas in order to obtain financial benefits. Faced with such facts as a means of authentication wide in the digital world aroused the interest of the famous social engineers, which uses specific techniques to obtain relevant information to the detriment of others. The Brazilian Federal Government implemented a linked hierarchy infrastructure Public Key called ICP Brazil, aiming to make emissions more secure digital certificates, however, this hierarchy suffers daily with attempts to executest fraud by social engineers. This research aims to understand the techniques used by social engineers when issuing digital certificates, using scientific methodology as the hypothetical deductive method, and the search classified as basic research, qualitative, descriptive, bibliographical and documentary. The world has evolved into digital, being necessary to protect the greatest asset an organization has: information. However, despite the implemented safety procedures, social engineers always look for gaps in the system to achieve its purpose. Therefore, to make effective security policies, they must be constantly evolving, following the human evolution.

Keywords: Information Security; Digital Certificate; Social Engineering.

SUMÁRIO

INTRODUÇÃO

Para Fontes (2006), a segurança da informação deixou de ser um item de luxo das pequenas e grandes empresas, e passou a ser algo primordial na gestão das mesmas. É importante ter em mente que o mundo está se tornando digital, portanto torna-se necessário proteger as informações também no meio digital, garantindo a autenticidade e integridade dos dados trafegados e das informações armazenadas**.**

Salienta o autor que grandes e pequenas organizações tiveram dados importantes roubados ou corrompidos pela falta de segurança implementada em seus sistemas ou de terceiros, se tornando alvo fácil de ataques maliciosos causando grande impacto nos negócios. Com tantas transações online percebe-se a necessidade de que uma pessoa pudesse autenticar-se em um sistema ou no meio digital, garantindo o não repúdio daquela ação.

A partir das necessidades, de: proteger informações no meio digital e validar documentos no meio computacional, nasceu à certificação digital, que é capaz de oferecer assinatura digital, *email* criptografado, nota fiscal eletrônica e outras funcionalidades, agregando maior segurança às transações. (MONTEIRO, MIGNONI. 2007)

Gouvêa (acesso em: 27/11/2014) destaca que hoje em dia não existem razões para que um grande número de papéis seja armazenado em uma sala, por se tratar de uma época em que a tecnologia é capaz de garantir a integridade do documento e das informações contidas, armazenando tudo em um espaço bem menor.

Fontes (2006) ressalta a importância dos backups (cópias de segurança), pois uma vez que uma informação for destruída, e não houver uma cópia de segurança da mesma, ela nunca mais será recuperada.

Reforçando as palavras de Gouvêa, Ferreira e Araújo (2006) salientam que a norma NBR ISO/IEC 17799, prevê que técnicas e sistemas criptográficos sejam

necessários para a proteção de informações que são consideradas de risco e, para as quais outros controles de proteção não oferecem proteção adequada.

Lucca e Filho (2005) dizem que o certificado digital possui uma grande magnitude, que até mesmo uma empresa possa ser vendida ou transferida de proprietário através de meios digitais, o que acaba por despertar interesses escusos em pessoas mal intencionadas.

Diante dessa realidade, destacam que foi necessário perceber que algumas políticas de segurança precisam ser implementadas no ato da emissão de um certificado, procurando evitar que fraudadores façam uso da engenharia social para conseguirem emitir um certificado fraudulento em nome de terceiros.

As autoridades certificadoras (AC) e autoridades de registro (AR) estão dentro de uma hierarquia vinculadas a Infraestrutura de Chaves Públicas do Brasil (ICP Brasil) e ao Instituto de Tecnologia da Informação (ITI), elas são responsáveis pela emissão de certificados e pelas políticas de segurança implementadas para evitar fraudes durante a emissão, porém ainda é necessário evoluir nesse campo visando aumentar a segurança relacionada aos certificados digitais. (LUCCA, FILHO, 2005)

O escopo desse trabalho limita-se a estudar fraudes ocorridas na emissão de um certificado digital e, estudar os métodos que os estelionatários usam para burlar a lei e fraudar certificado digital.

Para tanto, o estudo se **justifica** em função das necessidades que o mundo atual faz da aquisição de um documento eletrônico (certificado digital), existem alguns problemas fundamentais que estão basicamente ligados a três requisitos: Autenticidade, sendo ela referente à possibilidade de se identificar com elevado grau de certeza, a integridade que deve garantir a certeza de que o documento eletrônico não foi adulterado e, a perenidade de conteúdo, que se refere a sua validade ao longo do tempo (LUCCA, FILHO, 2005).

A aquisição de um certificado digital no ambiente ICP Brasil (Infraestrutura de chaves públicas brasileiras) é feita junto a uma Autoridade Certificadora. No

momento da validação presencial essa Autoridade Certificadora confirma se os dados contidos nos certificados são realmente pertinentes ao solicitante do certificado (FONTES, 2008).

Diante dessa realidade, pretende-se estudar e explorar o tema proposto, para obter-se conhecimento da amplitude e seriedade do certificado digital, além de ampliar o conhecimento referente à área de estudo, bem como para ampliar oportunidades de detecção na área por parte da aluna pesquisadora.

Já o **Problema** foi: Toda a hierarquia vinculada a ICP Brasil sofre, diariamente, diversas tentativas de emissão de certificado digital fraudulento tanto de pessoas físicas quanto as jurídicas através de estelionatários que fazem uso da engenharia social para atingir seus objetivos.

De acordo com o Sindicato das Empresas de Seguros, Resseguros e Capitalização (acesso em: 28/11/2014) Recentemente três tentativas de fraude foram notificadas pelo ITI: A primeira tentativa ocorrida na cidade de São Paulo, foi constatada após a emissão de um certificado e-CNPJ A1, sendo revogado após constatação de fraude, esse mesmo fraudador já foi alvo de diversas denúncias realizadas pelo ITI.

A segunda tentativa também ocorrida na cidade de São Paulo foi identificada através de um aviso da Caixa Econômica Federal, onde a vítima foi notificada da emissão de um certificado e-CNPJ em seu nome, que estava sendo utilizado para conectividade social, o certificado foi revogado e o alerta de tentativa de fraude encaminhado as autoridades de registro.

Na terceira tentativa de fraude também ocorrida na cidade de São Paulo, foi enviada a solicitação de um certificado digital a central de validação, porém foi constatado que esse mesmo fraudador já era alvo de diversas denúncias pronunciadas pelo ITI, gerando assim, a recusa do certificado digital solicitado pelo fraudador.

As autoridades de registro devem ter maior atenção no momento da validação de um certificado digital ICP Brasil, além de manter todos os registros de fraude para facilitar a identificação de possíveis fraudadores, anteriormente notificados pelo ITI, inibindo assim, a ação dos engenheiros sociais.

Como **Pergunta** que se buscou responder foi: Como proteger a certificação digital contra fraude e uso ilícito?

As **Hipóteses** foram: a) O usuário não precisa fazer nada, pois existe uma política padrão elaborada pelo ITI no que se refere às normas de segurança relacionadas à emissão de certificados digitais, porém cabe a cada autoridade certificadora implementar normas mais específicas para evitar a emissão de certificados fraudulentos; b) Mesmo com as políticas padrões elaboradas pelo ITI, o usuário não está protegido, pois hackers habilidosos quebram qualquer codificação, e c) Para aumentar o nível de segurança às autoridades de registro recebem notificações de tentativas de fraude, porém devem manter um repositório dessas notificações para que um mesmo fraudador não consiga emitir novamente um certificado digital fraudulento em prejuízo de um terceiro.

O **objetivo geral** consistiu em estudar os métodos utilizados pelos fraudadores quando da emissão de certificado digital, objetivando conhecer as técnicas da engenharia social utilizadas por eles.

Os **objetivos específicos** foram: a) Fazer um levantamento bibliográfico sobre segurança da informação (disponibilidade, integridade e confidencialidade) e a engenharia social, visando compreender as vulnerabilidades utilizadas pelos engenheiros sociais para que a segurança possa ser maior dentro desse campo; b) Estudar as certificações digitais, buscando identificar como as técnicas utilizadas pela engenharia social prejudicam os certificados digitais e, c) Discutir as questões teóricas estudadas a luz das fraudes relativas à emissão de um certificado digital com o uso da engenharia social, buscando analisar aspectos favoráveis e desfavoráveis no uso da certificação digital, para que seja possível compreender sua finalidade.

O **método** utilizado para o desenvolvimento deste trabalho foi o hipotético-dedutivo, que está relacionado ao “conhecimento que se obtém de forma inevitável e sem contraposição. Parte do geral para o particular, do conhecimento universal, para o conhecimento particular”. (FACHIN, 2006 p.32).

A **pesquisa** foi classifica da seguinte forma: Do ponto de vista e sua natureza foi utilizada a Pesquisa Básica, que “é aquela que procura o progresso científico, a ampliação de conhecimentos teóricos, sem a preocupação de utiliza-los na prática. É a pesquisa formal, tendo em vista generalizações, princípios, leis. Tem por meta o conhecimento pelo conhecimento.” (MARCONI, LAKATOS, 2011, p.6)

Para a abordagem do problema foi utilizada a Pesquisa Qualitativa: Uma vez que é: “multimetodológica quanto ao seu foco, envolvendo abordagens interpretativas e naturalísticas dos assuntos. Isto significa que o pesquisador qualitativo estuda coisas em seu ambiente natural, tentando dar sentido ou interpretar os fenômenos, segundo o significado que as pessoas lhe atribuem” (DENZIN & LINCOLN, 2006, p.2).

Para que os objetivos fossem atingidos utilizou-se a Pesquisa Descritiva, descrita por Marconi e Lakatos (2011, p.6) como aquela que: “Delineia o que é – aborda também quatro aspectos: descrição, registro, análise e interpretação de fenômenos atuais, objetivando o seu funcionamento no presente”.

Para os procedimentos técnicos utilizaram-se as Pesquisas: Bibliográfica e Documental. A pesquisa bibliográfica é aquela que dá “um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância por serem capazes de fornecer dados atuais e relevantes relacionados com o tema. O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar duplicações e certos erros, e representa uma fonte indispensável de informações podendo até orientar as indagações”. (MARCONI, LAKATOS, 2011, p.12).

Já a pesquisa documental é compreendida por Marconi e Lakatos (2011, p.12) como: “a análise minuciosa de todas as fontes documentais que sirvam de suporte a investigação projetada”.

O trabalho foi estruturado em **três** capítulos, sendo que o **primeiro** conceitua a segurança da informação e esclarece sobre sua importância para a gestão de negócios das organizações e, realiza uma introdução sobre a engenharia social, o **segundo** discorre sobre o avanço da tecnologia e as operações online, conceituando a engenharia social e sua relação com ataques aos certificados digitais. Com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior, o capítulo três se reserva às **Considerações Finais**.

1 SEGURANÇA DA INFORMAÇÃO E ENGENHARIA SOCIAL

A informação move o homem em todos os ambitos, e graças a ela foi possível evoluir-se ao longo dos anos, agregando maiores conhecimentos, e aprendendo através de tentativa e erro. O mundo tornou-se digital, e as informações antes manipuladas pelo meio físico, agora são trafegadas e armazenadas pelo meio digital.

Sendo assim, a Segurança da Informação deixou de ser um requisito opcional, tornando-se essencial a gestão de negócios de uma organização, principalmente, em se tratando de uma época que o uso da persuasão e empatia facilita para que os engenheiros sociais roubem informações vitais ao funcionamento de uma organização.

1.1 SEGURANÇA E INFORMAÇÃO

Sêmola (2003) afirma que segurança é um requisito que não pode faltar dentro de uma organização independente de seu porte, uma vez que ela visa proteger o maior e mais importante ativo dentro de uma empresa, a informação.

Acrescenta que se as regras necessárias para gerir a segurança não forem aplicadas, ou forem aplicadas parcialmente, as informações tanto no meio físico quanto no meio digital vão ficar vulneráveis a possíveis ataques, segundo uma analogia simples do próprio autor, é o mesmo que proteger a porta de entrada de uma residência com todos os recursos disponíveis, e se esquecer da entrada dos fundos da mesma residência, uma vez que brechas no sistema são utilizadas para atingir seu propósito final.

“Conceitos de segurança: Conceitos sólidos e seu claro entendimento são a matéria-prima que implicará na qualidade e no resultado dos trabalhos”. (SÊMOLA 2003 p.75)

Destaca o autor que diante da evolução do homem e também da revolução industrial que aconteceu ao longo da história é possível notar e compreender que a informação é o que move o homem, a evolução em todos os âmbitos, ela sempre esteve presente e foi fator principal para a gestão de negócios. O conceito de

informação está de forma importante ligada à evolução das empresas e dos negócios ao longo da história, independente do ramo de mercado adotado, ela apresenta todos os dados relativos a uma organização, que pode determinar o sucesso ou fracasso do negócio. Demorou um pouco para que o conceito de Tecnologia da Informação fosse difundido no mercado, esse conceito teve início com a entrada dos poderosos mainframes, e mais adiante surgiram às redes de computadores que foram capazes de otimizar cada vez mais rápido esse processo, nascendo, assim, o conceito de Tecnologia da Informação. A partir desse momento todas as empresas, independente de seu porte começam a fazer uso das informações no meio digital para a prospecção e crescimento do negócio, diante dessa visão percebe-se a dependência que as empresas têm da informação, e consequentemente da infraestrutura que mantém essas informações. (SÊMOLA, 2003)

Para Fontes (2006), a informação é o termo chave de uma organização, ela não possui um valor estimado, mas é crucial para o funcionamento da mesma, à medida que funcionários e colaboradores necessitam dela para realizar todas as tarefas pertinentes à empresa, torna-se de extrema importância que a mesma seja protegida.

Destaca o autor que a importância do armazenamento e proteção contra roubo, uso ilícito, e até mesmo a ações do tempo que também levam uma organização a perder informações cruciais. Uma vez perdida as informações, dificilmente será possível realizar a recuperação das mesmas na integra, o que pode impactar de forma severa uma organização, podendo levar até mesmo a falência.

> A informação, independentemente de seu formato, é um ativo importante da organização. Por isso, os ambientes e equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos. A informação tem valor para a organização. Sem informação, a organização não realiza seu negócio. (FONTES, 2006, p.1).

1.2 SEGURANÇA DA INFORMAÇÃO

> Podemos definir segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra

> acessos não autorizados, alterações indevidas ou sua indisponibilidade. (SÊMOLA, 2003 p.43)

Prado e Souza (2014) explicam que a Segurança da informação consiste basicamente na proteção dos ativos de uma organização, contra roubo, danos e perdas, aplicada diretamente a todas informações armazenadas, manipuladas ou transmitidas entre uma ou mais organizações.

Com o avanço da tecnologia, praticamente todas as informações referente a pessoas e organizações estão armazenadas no meio computacional. É de responsabilidade das organizações fazer bom uso e proteger os dados armazenados em seus sistemas, jamais se esquecendo de proteger também o ambiente físico onde os recursos se encontram implementados, uma vez que a segurança da informação trata tanto do aspecto físico como do computacional, sempre com o intuito de proteger as informações e garantir a continuidade do negócio. (FONTES 2006)

De acordo com Sêmola (2003), pode-se notar a importância da informação para a continuidade do negócio, tendo em mente que a informação deve ser preservada e protegida, e que a segurança da informação é ligada aos seus três pilares básicos:

> Confidencialidade: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para que elas são destinadas.
>
> Integridade: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
>
> Disponibilidade: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade. (SÊMOLA, 2003, p.45).

O autor ainda afirma que o ideal é estudar o desafio de proteger as informações através de camadas, ou seja, as seis barreiras da segurança, todas elas com o foco de reduzir os riscos dentro de um ambiente sendo elas: desencorajar, dificultar, discriminar, detectar, deter e diagnosticar.

Usuários finais devem ter consciência da necessidade de proteção relativa às informações e dados da empresa, uma vez que as organizações, muitas vezes, investem em segurança relativa às suas máquinas principais, por exemplo, servidores e switches, e não tem o mesmo nível de proteção relativa às máquinas dos usuários finais que realizam o acesso e faz uso dessas informações armazenadas, o que gera grande falha na proteção de informação. (FONTES 2006).

1.2.1 Políticas de Segurança

Fontes (2006) defende a ideia de que os funcionários devem ter em mente que a informação é muito maior “do que um conjunto de dados”, e que para protegê-las, uma série de normas e políticas devem ser estabelecidas, visando sempre proteger esses dados integralmente, para evitar todas as formas possíveis que sejam perdidos ou corrompidos por falha técnica, pela ação do homem ou do tempo.

O autor ainda reforça que além dos três pilares básicos existem outros três que também são utilizados no que se refere à segurança da informação, sendo eles:

- Legalidade: O uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como com os princípios éticos seguidos pela organização e desejados pela sociedade.

- Auditabilidade: O acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.

- Não repúdio de auditoria: O usuário que gerou ou alterou a informação (arquivo de texto ou mensagem de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem a sua autoria. (FONTES, 2006, p.12)

  Quando uma organização define uma política de segurança, seu objetivo é explicitar aos usuários que acessam e utilizam a informação qual é a filosofia e quais são as regras sobre esse recurso. A organização busca garantir que a informação esteja protegida contra possíveis perdas, danos, destruição e mau uso. (FONTES, 2006, p. 12 e 73).

Ferreira e Araujo (2006) reforçam a ideia de Fontes afirmando que com o intuito de proteger a informação dentro de uma organização uma política de segurança deve ser elaborada e implementada por auditores, para tanto, é necessário entender as necessidades da organização, uma vez que regras

diferentes se aplicam a empresas diferentes, visando todos os aspectos e, em qual departamento se encontram os ativos que necessitam de maior proteção, lembrando que o maior risco está sempre relacionado ao fator humano, ou seja, o usuário final.

Fontes (2008) afirma que a política de segurança deve sempre estar alinhada aos objetivos dos negócios, para tanto as organizações devem fazer uso dos recursos necessários de forma que sejam possíveis desenvolverem suas formas de negócios, sem prejudicarem a segurança da informação ou a viabilidade dos negócios.

Ferreira e Araujo (2006) relatam em sua obra que, a partir do momento em que uma organização opta por implementar políticas de segurança torna-se necessário definir a equipe responsável, que deve ter por base a alta administração da empresa, podendo, assim, definir as melhores políticas, medidas e sanções a serem implementadas.

Os autores explicam ainda que a política de segurança deve abranger todos os aspectos referentes à segurança física e virtual das informações e dos equipamentos instalados dentro de uma organização. Cada aspecto deve ser levantado e avaliado dentro desse contexto, sempre tendo em mente que o usuário é o elo mais fraco relativo à segurança da informação. Com essa visão, a estrutura organizacional deve ser avaliada pelos auditores juntamente com uma equipe do alto escalão definida pela diretoria, selecionada dentro da empresa, que abranja todos os setores para que sejam definidos os ativos e recursos de maior importância. Treinamentos em todos os setores devem ser feitos com frequência para maior conscientização dos colaboradores, um documento específico sobre as políticas adotadas pela empresa deve ser redigido e apresentado ao quadro de funcionários, para que seja de conhecimento geral todas as normas estabelecidas sempre com o intuito de planejar a continuidade dos negócios diante de um possível evento negativo.

Fontes (2006) explica que, a partir do momento em que novos colaboradores são admitidos, seria necessário que um termo de conscientização e confidencialidade seja redigido e assinado com o intuito de passar aos novos

funcionários as políticas vigentes no que se refere à proteção da informação e também para que o mesmo tenha consciência das ações e medidas necessárias para proteger a empresa de um possível ataque ou vazamento de informações.

Sêmola (2003) afirma que as políticas de segurança devem estar alinhadas ao plano de negócios e que exames e testes superficiais devem ser aplicados para que seja possível diagnosticar possíveis ameaças, vulnerabilidades e riscos potenciais. Deve-se levar em conta toda a infraestrutura física, tecnológica e humana, não é uma tarefa simples, principalmente quando se analisa uma empresa de grande porte, mas essa etapa é muito importante, pois, auxiliam a elaboração de uma política com visão no plano de continuidade dos negócios.

Ferreira e Araujo (2006) reforçam a visão de Sêmola de que é necessária a elaboração de um plano de continuidade que seja capaz de orientar um possível processo de restauração em caso de algum desastre de ordem intencional ou natural. O plano de continuidade deve conter as diretrizes necessárias que orientem como proceder em cada situação, que deve estar alinhado com a gestão de riscos, de forma que os riscos mapeados estejam parcialmente ou totalmente suportados.

Entre as políticas para autenticação do usuário que devem ser estabelecidas, a mais utilizada atualmente é a senha, que deve ser pessoal e intransferível, além de contar com uma política mínima para cadastro da mesma, exigindo sempre senhas alfanuméricas contendo símbolos e letras maiúsculas, não permitindo que o usuário cadastre data de nascimento, número de telefone ou senhas sequenciais. (FONTES, 2006)

O autor lembra ainda que outro ponto importante relacionado a permissões de acesso está ligado ao fato da necessidade da exclusão imediata do acesso aos sistemas dos funcionários que já se desligaram da organização, ou de colaboradores já falecidos, uma vez que pessoas mal intencionadas podem fazer uso dessas permissões para acessar informações de uma organização indevidamente, portanto, independentemente do cargo exercido, também é importante implementar datas onde esse acesso seja expirado e um novo precise

ser gerado. Também é de extrema importância armazenar *logs* de acesso para controlar e monitorar as ações dos usuários.

O autor explica que atualmente existe uma forma de autenticação no sistema e meio computacional chamado de certificado digital, com a instalação do mesmo em um computador ou mídia própria para armazenamento é possível se autenticar no sistema ou meio digital, garantindo a identificação e autenticação do usuário. O certificado digital contém suas informações pessoais e um par de chaves que garantem maior segurança para acesso e autenticação no sistema, esse tema será abordado profundamente mais adiante.

Fontes (2006) complementa que nas regras de acesso da política de segurança é importante permitir acesso ao usuário apenas aquilo que é essencial para ele realizar suas funções, para que isso seja feito é importante que a equipe de gestores realize a nomeação de um gestor de informação, que será o profissional responsável por liberar ou restringir acessos dentro de uma organização. Também é necessário que os usuários tomem algumas medidas de precaução para evitar possíveis transtornos, tais como o não compartilhamento de senhas e informações pertinentes à organização.

Prado e Souza (2014) explicam que o erro humano é uma forte vulnerabilidade dentro de uma organização, e que os motivos podem ser dos mais variados, dentre eles, sobrecarga de trabalho, urgência, fadiga ou desmotivação. Em muitos casos o erro humano é derivado da falta de conhecimento das políticas internas, pois não existe comunicação correta da organização perante seus colaboradores.

Fontes (2006) ressalta que dentro da política de segurança é fundamental a realização de backups (cópias de segurança), caso algum sistema entre em pane, ou informações sejam perdidas por ação do tempo ou mal uso de usuários, o backup deve evitar perda de informações, ou ao menos minimizar esse impacto, porém essas cópias de segurança devem ser mantidas em locais seguros e longe da organização física, pois diante de um desastre natural ou provocado intencionalmente a sede física, a cópia das informações serão mantidas intactas.

Relata o autor, dois casos bem específicos onde informações cruciais foram perdidas por falta de um sistema de backup bem elaborado, sendo elas:

Um caso bem específico de grande perda de informações, com forte impacto no mercado relacionado a backups foi o ataque ao World Trade Center. Todos os backups eram replicados do servidor de um prédio para o outro, como o ataque atingiu ambos os prédios todas as informações foram perdidas, levando meses para recupera-las parcialmente, com o efeito dominó diversas empresas declararam falência, uma vez que informações cruciais a existência das mesmas foram perdidas no momento do ataque. Atualmente para evitar este tipo de transtorno, grandes e médias organizações tem cópias de seus backups em continentes diferentes, aumentando assim a redundância. (JORNAL O GLOBO, 2002, apud, FONTES).

Outro exemplo relacionado a grande perda de dados importantes é o incêndio que ocorreu na Universidade Federal do Pará onde anos de pesquisa foram consumidos pelo fogo, o cálculo do prejuízo é inestimável, mais de dez anos de pesquisa foram perdidos, uma vez que as informações estavam em papel e não possuíam nenhuma cópia de segurança, por isso é imprescindível o uso de cópias de segurança periodicamente. (ESTADÃO, 2003, apud, FONTES)

Sêmola (2003) lembra que é importante implementar algumas medidas de segurança para minimizar impactos, são consideradas controles, tendo elas as seguintes características:

> Preventivas: Medidas de segurança que tem como objetivo evitar que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança da instituição.
>
> Detectáveis: Medidas de segurança que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades.
>
> Corretivas: Ações voltadas a correção de uma estrutura tecnológica e humana para que as mesmas se adaptem as condições de segurança estabelecidas pela instituição, ou voltadas à redução dos impactos:equipes para emergências, restauração de backup, plano de continuidade operacional, plano de recuperação de desastres. (SÊMOLA, 2003, p.49)

Prado e Souza (2014) reforçam da importância da instalação de antivírus nas máquinas. Os programas de antivírus servem para notificar ou bloquear parcialmente a ação de arquivos executáveis que acessam a máquina através da rede de internet, seja por acesso a sites mal intencionados, ou abertura de e-mails maliciosos, a finalidade de um vírus de computador é sempre executar ações de má fé. Os vírus de computador já atacaram diversas máquinas ao redor do mundo, suas vítimas vão desde pessoas comuns até grandes organizações. Para tornar mais efetiva a ação dos programas de antivírus é necessário atualizar o programa sempre com a versão mais recente, e realizar varreduras periodicamente. Porém é importante a conscientização de usuários, que acreditam ter perda de desempenho do equipamento perante a utilização de antivírus, e acabam por desligar em determinadas circunstâncias, o que pode impactar a segurança da organização.

Fontes (2006) reforça que o correio eletrônico é uma ferramenta que deve ter suas regras de acesso estabelecidas pela política de segurança, uma vez que seu uso deve ser de caráter profissional, sempre com o intuito de manter a boa imagem da organização. Atualmente existem diversas soluções que conferem maior segurança relacionada ao envio de e-mails garantindo maior confidencialidade, uma vez que fraudadores fazem uso de e-mails com a intenção de roubar informações.

Um caso de tentativa de ataque através de um arquivo executável enviado através de um e-mail intitulado como sendo do Instituto Brasileiro de Geografia e Estatística (IBGE) foi enviado a diversas famílias, o caso foi encaminhado a Polícia Federal (ESTADO DE SÃO PAULO, 2005, apud, FONTES).

O autor acredita que a legislação vigente atualmente cobre parcialmente crimes de caráter virtual, mas as organizações e empresas devem ter implementadas ações para a proteção das informações no meio virtual, sempre com o intuito de minimizar ao máximo ações com intenções maliciosas.

De acordo com a gerente de estratégias de segurança da Microsoft Brasil Anna Carolina Aranha (apud MICROSOFT, acesso em: 23\02\2015) o conceito de segurança da informação ganhou maior visibilidade na atualidade, mas manter registros de informações codificadas remete desde os tempos remotos, uma vez que

até mesmo os egípcios da antiguidade faziam uso da codificação em mensagens e registravam as informações de sua época. Segurança da informação não depende apenas das políticas estabelecidas dentro de uma empresa para ser eficaz, para tanto, é necessário leis mais rígidas com o intuito de alcançar esse fim.

Aranha (apud MICROSOFT, acesso em: 23/02/2015) também informa que as atualizações dos softwares são essenciais para evitar possíveis ataques, de nada adianta realizar um alto investimento em segurança se itens indispensáveis como configuração e atualização de software não estiverem perfeitamente alinhados, uma vez que hackers habilidosos fazem uso dessa falha para invadir um sistema.

Fontes (2006) reforça que todos os países possuem leis relacionadas a privacidade, obviamente em determinados países essas leis são ou não mais desenvolvidas. No meio profissional é imprescindível implementar políticas de privacidade tanto no meio virtual, quanto no meio físico. Cada organização deve ter suas políticas de privacidade estabelecidas de acordo com a necessidade do negócio, porém respeitando a privacidade das informações relacionadas a seus clientes. Da mesma forma, colaboradores e funcionários não podem divulgar informações privadas da organização, todos esses requisitos devem estar estabelecidos na política de segurança da empresa.

Em abril de 2005 um banco japonês assumiu a perda de informações de aproximadamente 270.000 clientes, esse mesmo banco assumiu ter enfrentando certa dificuldade na integração dos dados, aparentemente os dados foram simplesmente descartados, o que gera grande desconforto, uma vez que números de contas, valores em depósitos e outras informações confidências compunham o disco descartado erroneamente. (JORNAL O ESTADO DE SÃO PAULO, 2005, apud, FONTES).

Informações de clientes armazenadas em servidores e bancos de dados de uma corporação devem ser específicas e restritas ao que se faz necessário dentro da organização. Eles são responsáveis pelas informações armazenadas, e quando em mãos de pessoas mal intencionadas pode gerar mais do que desconforto. (FONTES, 2006).

Ferreira e Araújo (2006) explicam que obviamente, não é possível definir de forma generalizada as ações que devem ser tomadas dentro de uma organização no que se refere as políticas de segurança, uma equipe de auditoria deve ser contratada para verificar todos os pontos vulneráveis, além de definir a gestão do risco de acordo com as atividades exercidas por cada organização juntamente com a equipe definida dentro da organização, porém foi abordado de forma geral pontos específicos da segurança da informação, definindo algumas ferramentas e implementações necessárias para que a continuidade do negócio não fosse impactada diante de um possível ataque.

1.3 ENGENHARIA SOCIAL

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem uso da tecnologia. (MITNICK, SIMON 2003, Prefácio)

De acordo com a Revista Gestão de Riscos (2011) uma ameaça fraudulenta crescente, os autores Lennert e Oliveira afirmam que o termo engenharia social vem sendo amplamente abordado por alguns segmentos das indústrias, uma vez que utilizam-se de falhas humanas para atingir suas finalidades, de acordo com os autores o assunto vem ganhando ênfase uma vez que, as empresas tem por objetivo conscientizar seus funcionários, pois ataques de engenharia social afetam setores críticos de uma organização, de acordo com eles essa tática pode ser entendida como um ataque que faz uso da manipulação do psicológico das pessoas.

Peixoto (2006) afirma que desde os tempos remotos o homem faz uso da persuasão para obter seus fins, isso se demonstra ao longo da história e até mesmo na bíblia, um exemplo claro é quando a serpente convenceu Eva a provar do fruto proibido, utilizando-se da influência e da manipulação para obter seu fim. Com o engenheiro social ocorre basicamente a mesma coisa, ele foca naquilo que precisa obter e usa o conhecimento do comportamento humano para obter esse fim.

O autor também relata uma definição utilizada por um dos maiores engenheiros sociais que já existiu, o famoso Kevin Mitnick se refere a engenharia social como "um termo para definir o uso da persuasão para influenciar as pessoas a

concordar com um pedido". O engenheiro social é na maioria das vezes, simpático e extrovertido, carismático, mas nem toda engenharia é usada para fins prejudiciais, promotores, investigadores e advogados fazem uso da engenharia social para obterem seus fins. Os engenheiros sociais estão constantemente inovando suas técnicas para acessar ou obter aquilo de que precisam.

Peixoto (2006) explica que nem todo engenheiro social é uma *hacker*, ou vice e versa, sendo *hacker* um termo utilizado para designar alguém que acessa de forma indevida informações através de um recurso computacional, e engenheiro social, alguém que utiliza-se de técnicas de persuasão para atingir seus objetivos. Porém *hackers* podem fazer uso da engenharia social para coletar informações pertinentes a pessoas e organizações com o intuito de atingir seus objetivos.

Fontes (2006) define a engenharia social como o uso da persuasão para a coleta de informações cruciais de uma organização, usando de simpatia e criando empatia com as pessoas, o engenheiro social consegue obter as informações necessárias sem fazer uso de força bruta para obtê-las.

Destaca que eles possuem uma personalidade peculiar, que procuram falar com certa familiaridade sobre os assuntos abordados, sempre procura se passar por amigo, familiar ou conhecido de alguém importante, e também procura falar com conhecimento sobre a organização, dessa forma ganha a confiança de outras pessoas, às vezes até mesmo em longo prazo, sem pressa ele consegue as informações de que necessita.

Mitnick e Simon (2003) afirmam que o usuário é sempre o elo mais fraco de uma organização, a mesma pode investir em todos os recursos mais sofisticados de segurança, mas, ainda assim uma empresa vai estar vulnerável devido ao fator humano. Eles descrevem o engenheiro social como um mágico inescrupuloso que engana as pessoas para alcançar o seu objetivo.

Há quem diga que um computador seguro é um computador desligado, porém Kevin Mitnick reforça que essa frase não é inteiramente verdadeira, uma vez que um bom engenheiro social pode conseguir informações de um usuário de confiança que

tenha acesso a informações relevantes de uma organização, até mesmo faz uma analogia, afirmando que, assim como os analistas de criptografia são capazes de revelarem um texto simples criptografado, os engenheiros sociais enganam usuários para escapar da tecnologia da segurança da informação.

Peixoto (2006) afirma que os engenheiros sociais estão em constante inovação no que diz respeito às técnicas utilizadas para obter sucesso no acesso e roubo de informações. Mas como definir o que são ou não informações importantes para uma organização? Um funcionário despreparado não pode definir essa questão e pode acabar liberando informações sigilosas para pessoas mal intencionadas.

Lennert e Oliveira (2011) explicam que existem diversas maneiras de trabalhar com a engenharia social, na sua maior parte usando o fator humano, Kevin Mitnick *hacker* e engenheiro social extremamente conhecido no meio afirma que é muito mais simples conseguir uma senha através da engenharia social, atacando o ponto fraco que é o psicológico, do que fazendo uso de programas para decodificar senhas. É importante ressaltar que nem todo engenheiro social é um hacker, uma vez que o ataque pode ter diversas finalidades e fatores.

Fontes (2006) explica que com a sofisticação que a evolução no meio digital vem ganhando, cada vez se torna mais difícil se autenticar em um sistema para roubar informações, por isso o uso da engenharia social tem se tornado uma ótima alternativa.

O autor afirma que eles usam o conhecimento e linguagem de uma organização para alcançarem o seu fim, se passando por antigos ou novos funcionários, parentes de colaboradores entre outros. Tem por objetivo criar um elo com a vítima para obter o maior número possível de informações necessárias, sempre fazendo uso do conhecimento e da simpatia. Muitas vezes podem restringir algum acesso da vítima e depois se passarem por *help desk* (suporte) para ganharem a sua confiança. Obviamente empresas de maior porte são mais vulneráveis a esse tipo de ação, uma vez que é mais fácil se passar por outro colaborador. Pode parecer brincadeira, mas existem pessoas especializadas em engenharia social.

Reforçando as palavras de Fontes, Mitnick e Simon (2003) mostram em sua obra que para um engenheiro social obter sucesso em atingir o seu objetivo é necessário uma grande dose de conhecimento e habilidade relacionados aos computadores e a telefonia, e que para alcançar esse fim o engenheiro social vai manipular pessoas.

Peixoto (2006) afirma que os engenheiros sociais fazem uso da psicologia humana, usando medo ou piedade de outras pessoas como ferramenta para obter as informações de que precisam, até mesmo os colocam em uma situação em que a vítima pode dar informações acreditando que se não o fizer pode perder seu emprego.

Como já dito anteriormente, Peixoto (2006) mostra que o elo mais fraco de uma organização é o fator humano, isso é indiscutível, pois até mesmo Kevin Mitnick afirma esse ponto, por isso engenheiros sociais fazem uso deles para obterem as informações de que necessitam, normalmente, os funcionários trabalham com computadores, mas não percebem a importância que as informações armazenadas nesse meio têm para a continuidade do negócio de uma organização, os famosos engenheiros sociais, normalmente, fazem uso dessa falta de percepção e treinamento para conseguirem roubar as informações de que precisam, quando se trata de segurança da informação, a regra é sempre desconfiar.

> Se todo funcionário fosse tão questionador como uma criança, demonstrando interesse nos mínimos detalhes, ouvindo mais, estando fortemente atento a tudo à sua volta, e principalmente fazendo o uso dos poderosos "por quês", com certeza as empresas transformariam os frágeis cadeados em legítimos dispositivos dificultantes de segurança da informação (PEIXOTO, 2006, p. 20).

Pode-se perceber a fragilidade do fator humano com uma analogia bem simples, basta observar os aeroportos, constantemente terroristas conseguem burlar o sistema e adentrar em aeroportos e aviões com armas de fogo ou explosivo, mas como explicar essa questão, uma vez que a tecnologia referente a detecção desse tipo de equipamento está cada vez mais eficiente. A resposta é simples, o fator humano, por isso a informação deve ser protegida de todas as formas possíveis, uma vez que, continuarão a ser alvo dos atacantes que possuem a habilidade da engenharia social. (MITNICK, SIMON 2003).

Dentro do contexto abordado no primeiro capítulo, notamos a fragilidade que a segurança da informação possui principalmente, no que concerne ao fator humano, principal vulnerabilidade explorada pelos engenheiros sociais. Eles estão em constante evolução, acompanhando a inovação da tecnologia e aprimorando suas técnicas, portanto se um novo meio de autenticação através da internet conhecido por certificado digital está surgindo, sendo o mesmo obrigatório pelo Governo Federal do Brasil, obviamente os engenheiros sociais querem fazer uso dessa tecnologia em proveito próprio.

2 ESTUDO DAS CERTIFICAÇÕES DIGITAIS E AS TÉCNICAS UTILIZADAS PELOS ENGENHEIROS SOCIAIS

Com o avanço da tecnologia e as operações online, por questão da segurança da informação dos dados trafegados, foi necessário o desenvolvimento de um método seguro para a autenticação do usuário na internet, tanto de pessoa física como de pessoa jurídica, nascendo assim os certificados digitais. Porém toda essa tecnologia e facilidade atraiu a atenção de golpistas, que através da utilização de técnicas da engenharia social, roubam informações de pessoas e organizações com o objetivo emitir um certificado, em prejuízo de outro para obter vantagem pessoal e financeira.

2.1 CERTIFICAÇÕES DIGITAIS

2.1.1 Criptografia

Segundo Monteiro e Mignoni (2007), a criptografia é uma ciência que faz uso da matemática com o intuito de decifrar códigos e dados, sendo a palavra criptografia com origem grega, *Kriptus* que significa escondido, oculto e *grifo* significa escrita.

A Cartilha do Certificado Digital (acesso em: 07/04/2015), explica que a criptografia oferece uma tecnologia capaz de codificar textos transformando uma mensagem comum em mensagem cifrada, garantindo assim que somente pessoas autorizadas sejam capazes de realizar a decifragem dessa mesma mensagem através de um processo inverso ao da cifragem.

Não é possível estudar certificado digital sem antes entender basicamente como funciona a criptografia, existem dois tipos de criptografia, a simétrica que é realizada com uma única chave tanto para cifrar quanto para decifrar uma mensagem e, a assimétrica ou pública que é realizada por um par de chaves, a chave pública e a chave privada, ambas são geradas simultaneamente e relacionadas entre si, à chave privada deve ser mantida em sigilo, enquanto a chave pública pode ser disponibilizada. Sem o conhecimento da chave não é possível decifrar a mensagem codificada. (MONTEIRO, MIGNONI 2007.)

Monteiro e Mignoni (2007) explicam que o primeiro algoritmo assimétrico a ser desenvolvido foi o RSA, seu nome se deve as iniciais dos sobrenomes de seus três desenvolvedores, sendo eles Ron Rivest, Adi Shamir e Leonard Adleman. Foi o primeiro algoritmo capaz de proporcionar a assinatura digital, sendo o algoritmo mais popular, baseado na dificuldade em fatorar dois números primos grandes. Os ataques a esse tipo de algoritmo podem ocorrer por força bruta, onde o invasor tenta decifrar a mensagem codificada.

Os autores ainda afirmam que o nível de segurança estabelecido pela criptografia está diretamente ligado ao tamanho da chave, ou seja, quanto maior o número de bits que uma chave possuir, mais difícil será a decodificação dessa chave. Com relação a segurança a criptografia provê os seguintes serviços:

> Autenticação: Garante a origem da informação, permitindo sua comprovação.
>
> Integridade: Assegura a veracidade e a integridade da informação recebida.
>
> Confidencialidade: Garante o acesso as informações somente pelas pessoas autorizadas.
>
> Irretratabilidade: Assegura que a origem (o emissor) da mensagem não poderá negar que foi o autor de determinada mensagem. (MONTEIRO, MIGNONI, 2007, p. 6).

"A tecnologia da criptografia desenvolvida nos últimos 30 anos foi a principal responsável pelo desenvolvimento da certificação digital que oferece inúmeros benefícios aos seus usuários, agilizando procedimentos e diminuindo custos". (apud, CARTILHA DO CERTIFICADO DIGITAL, p.1 acesso em 07/04/2015).

2.1.2 Certificado digital

> O certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Ele pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital. (CARTILHA DE SEGURANÇA NA INTERNET, 2012 p.70).

Um certificado digital ou identidade digital é um arquivo digital que como os demais documentos físicos de identificação, contém os dados do indivíduo ou

entidade e possui também uma chave pública e privada associada ao assinante. Esse tipo de documento é chancelado digitalmente pela entidade emissora, denominada Autoridade Certificadora (AC), que tem por objetivo interligar uma chave pública a uma pessoa ou entidade, conferindo a esse certificado a mesma validade de um documento físico, porém no meio digital. (MONTEIRO, MIGNONI, 2007).

A Cartilha do Certificado Digital (acesso em: 07/04/2015), explica que a criptografia utilizada no que se refere aos certificados digitais é assimétrica, possui um par de chaves, a característica marcante desse par de chaves é que um texto criptografado com esse certificado vai usar uma chave para criptografar e a outra para descriptogtafar essa mesma mensagem. A chave privada é de conhecimento apenas do proprietário do certificado, sendo protegida por senha, enquanto a chave pública não possui esse tipo de restrição.

A tecnologia da certificação digital garante a confidencialidade, integridade e não repúdio que estão ligados aos pilares da segurança da informação na troca de mensagens eletrônicas possibilitando a segurança de troca de dados. A certificação digital é um documento eletrônico que contém o nome e a chave pública e privada permitindo que pessoas se autentiquem nos sistemas, comprovando a autenticidade para pessoas e sistemas. O certificado digital é responsável por cumprir a função de validar alguém no meio digital associando uma pessoa ou entidade a uma chave pública. (MONTEIRO, MIGNONI. 2007)

Os autores explicam que existem informações mínimas que devem constar dentro do arquivo digital relacionado aos certificados, esses dados são: Chave pública, nome do proprietário ou entidade, número de série do certificado, nome da AC responsável pela emissão, assinatura digital da AC. Além dessas informações, caso considere necessário a AC pode acrescentar outras informações pertinentes.

A Cartilha do Certificado Digital (acesso em: 07/04/2015), explica que os certificados digitais podem garantir maior facilidade nas ações e transações, proporcionando maior agilidade aos procedimentos burocráticos, mas essa facilidade não isenta seu usuário, uma vez que ele garante o não repúdio das

informações, tornando assim o usuário responsável pelas ações tomadas durante o uso do certificado digital.

Por isso é importante que o usuário seja capaz de armazenar essas informações de forma segura. Alguns dispositivos como o *Smart card ou e-token* são uma espécie de *hardware* criptográfico capaz de armazenar seu certificado digital em um ambiente seguro. (MONTEIRO, MIGNONI. 2007)

Os autores complementam que alguns tipos de certificados digitais armazenam as chaves na própria máquina sendo esses conhecidos como tipo A1, mas para tanto é aconselhável que algumas medidas de segurança sejam tomadas, como, gravar senha de acesso, não utilizar dados pessoais como senha, caso o mesmo seja instalado em um ambiente com várias pessoas criar recursos de controle de acesso, manter atualizado sistema operacional e aplicativos e não instalar em computadores de uso público.

Segundo Fontes (2008) Quando existe comunicação com outra pessoa presencialmente ou através de meios tecnológicos partimos da premissa que aquela pessoa é quem diz ser, e que a mensagem enviada e recebida não foi alterada, que somente os interlocutores daquela mensagem terão acesso a ela, e que as informações trocadas não podem ser negadas. Dependendo o nível de comunicação necessário esse tipo de mensagem é suficiente, porém em ambientes corporativos onde esse contato é feito fora do ambiente organizacional, ou referente a transações bancárias esse tipo de comunicação acaba sendo falha, pois para tal procedimento é necessário um nível de segurança onde a identidade do interlocutor seja garantida, a garantia de não repúdio das informações trocadas, a garantia de que as informações trocadas estejam integras e não possam ser alteradas, e que essas informações sejam sigilosas, garantindo que apenas pessoal autorizado tenha acesso a elas. O certificado digital é capaz de garantir esse tipo de exigência, tornando mais segura as ações realizadas no meio computacional.

A Cartilha do Certificado Digital (acesso em: 07/04/2015), explica que os bancos são um ótimo exemplo relacionado ao uso de certificados digitais, eles usam os certificados para autenticar-se perante o cliente, garantindo que todos os dados

estão sendo enviados e recebidos de um servidor do banco. Órgãos governamentais também fazem uso dos certificados digitais, visando à redução de custos, agilidade nos processos, menor burocracia e maior facilidade para os usuários.

Mas atente-se em relação ao uso dos certificados digitais, a Cartilha de Segurança na Internet (acesso em: 07/04/2015),apresenta que alguns pontos devem ser observados em relação aos certificados para garantir a sua confiabilidade, primeiro é necessário verificar se a AC responsável pela emissão é confiável, se o certificado digital está dentro do prazo de validade, devem-se conferir os dados e também a entidade a qual está vinculada, além de conferir se esse certificado consta na lista de certificados revogados. A chave pública pode ser amplamente divulgada, porém é necessário comprovar a quem ela pertence, pois você pode se comunicar com um impostor e não perceber.

Monteiro e Mignoni (2007) orientam que é possível revogar o certificado digital antes que ele expire, os motivos podem ser os mais variados, como comprometimento de chave privada, alteração de dados, fraude, entre outros, para efetuar essa ação o usuário deve se reportar a AC responsável pela emissão de seu certificado digital. Quando a AC recebe a solicitação de revogação o número de série do certificado é adicionado a lista de certificados revogados, essas listas devem ser publicadas e podem ser consultadas para a verificação se um certificado se encontra ativo ou não. Após a revogação todas as assinaturas realizadas com esse certificado se tornam inválidas, porém assinaturas realizadas antes da revogação continuam válidas. O certificado digital possui data de vencimento pois a cada renovação, é possível renovar também a relação de confiança entre AC e usuário, além de oferecer novas tecnologias implementadas e tornar a segurança em relação a emissão de certificados digitais mais robusta.

Em caso de suspeita do comprometimento da chave privada do certificado digital, é essencial que seja solicitado junto a AC responsável pela emissão a revogação do certificado digital, garantindo assim que mais ninguém tenha acesso ao mesmo. (CARTILHA DO CERTIFICADO DIGITAL, acesso em: 07/04/2015)

Segundo Fontes (2008) caso o certificado digital tenha sido emitido por uma AC vinculada a cadeia da ICP Brasil, o mesmo possuirá validade jurídica. Um dos empecilhos relacionados ao uso do certificado digital são o custo e a exigência de ser necessária a emissão de vários certificados digitais, mas com a evolução nesse campo e os benefícios decorrentes da sua utilização, é apenas questão de tempo até esses contratempos serem resolvidos.

Ele ainda reforça que apesar do foco relacionado ao uso de certificado digital relacionado a pessoas, existem certificados para diversos outros recursos, como sites de internet, softwares, entre outros.

O certificado digital pode ser comparado a seu documento de identificação, como o RG ou passaporte, ele garante sua identificação no meio digital, e o órgão responsável pela sua emissão é uma autoridade certificadora (CARTILHA DE SEGURANÇA NA INTERNET, 2012)

2.1.3 Assinatura digital

Quando um documento impresso é assinado, está ocorrendo a autenticação referente a assinatura e aos dados contidos nesse documento, contendo nessa assinatura as biocaracterísticas de seu assinante. Nos documentos eletrônicos não existe esse tipo de autenticação física. A assinatura digital é um algoritmo de autenticação, que possibilita ao responsável unir a um objeto criado um código que deve agir como a assinatura desse documento digital (MONTEIRO, MIGNONI. 2007).

Ferreira e Araujo (2006) afirmam que um dos benefícios oferecidos pela criptografia assimétrica é o uso da assinatura digital, que é capaz de garantir a autenticidade e integridade das informações fornecidas, além de garantir o não repúdio das informações prestadas.

A Cartilha do Certificado Digital (acesso em: 07/04/2015), reforça que a criptografia de chave pública garante a confidencialidade e a autenticidade das informações por elas criptografadas. Os algoritmos de criptografia também permitem que seja realizada a assinatura digital. Isso garante que o documento não sofra

nenhuma alteração, pois o *hash* cifrado com a chave privada é anexado ao documento. A assinatura digital confere maior segurança a assinatura de documentos eletrônicos validando o usuário através do meio digital. Em agosto de 2001 a medida provisória 2.200 garantiu a validade jurídica da assinatura digital e do uso de certificados digitais, tornando assim a assinatura digital válida juridicamente.

Fontes (2008) explica que o governo federal já legalizou a Infraestrutura de Chaves Públicas do Brasil (ICP Brasil) e conferiu validade legal e jurídica a documentos eletrônicos assinados digitalmente, sendo assim vai chegar ao ponto onde todos os cidadãos, instituições, organizações entre outros vão se ver obrigados a fazer uso da assinatura digital.

> Assinar um documento é a transformação da informação de um documento para um resumo numérico, por meio da utilização de uma função matemática e da criptografia desse resultado com a chave privada da pessoa que assina. (FONTES, 2008 p.151).

Monteiro e Mignoni (2007) explicam que a assinatura digital permite a verificação de que o documento assinado não foi alterado desde sua criação, permitindo reconhecer seu assinante, garantindo assim a autenticação.

A Cartilha do Certificado Digital (acesso em: 07/04/2015), instrui que um certificado digital possui prazo de validade, portanto para assinar digitalmente os documentos eletrônicos é necessário que o certificado digital esteja válido, mas mesmo após seu vencimento é possível verificar a validade de documentos eletrônicos assinados por ele anteriormente.

2.1.4 Hierarquia ICP Brasil

Todos os serviços válidos juridicamente relacionados a certificação digital pública, são implementados por uma hierarquia de Infraestrutura de Chaves públicas conhecida como ICP Brasil. (MONTEIRO, MIGNONI. 2007)

Os autores explicam que a ICP Brasil possui uma série de padrões e normas a serem seguidas, sendo eles um conjunto de serviços necessários para que o uso de tecnologias baseadas em chaves assimétricas possa ser utilizado em grande escala. Para que a comunicação e transações eletrônicas possam se tornar viáveis

em todo o seu potencial, é necessário um alto grau de segurança, sendo os cinco requisitos a seguir essenciais para esta confiança:

> Autenticação: Garante a origem da informação, permitindo a comprovação da origem;
>
> Integridade: Assegura a veracidade e integridade da informação recebida;
>
> Confiabilidade: Garante o acesso as informações somente pelas pessoas autorizadas;
>
> Não repúdio: Garante que nem o emissor e nem o receptor da informação neguem a autoria ou o recebimento da informação;
>
> Autorização: Garante que uma determinada operação seja autorizada. (MONTEIRO, MIGNONI, 2007, p.14).

Dentro da hierarquia ICP Brasil, existe a autoridade certificadora raiz denominada Instituto Nacional de Tecnologia da Informação (ITI) que é o mais alto nível em uma cadeia de certificados, sendo ela responsável pela emissão de certificados para as ACs inferiores dentro da hierarquia. Alguns dispositivos de hardware são utilizados para criar, proteger, gerenciar e até destruir a chave privada referente ao certificado. Todas as ACs são relativamente subordinadas a outra AC, sendo ela a AC-Raiz. As ACs são responsáveis por emitir, gerenciar e revogar certificados dos usuários finais. Elas podem pertencer a uma entidade pública, ou a uma entidade privada. As Autoridades de Registro, dentro da hierarquia são as entidades responsáveis por solicitar, avaliar, aprovar ou rejeitar as solicitações de certificados, e dependendo do resultado encaminhar para a AC responsável. Toda AC deve manter um repositório disponível para o público com o intuito de armazenar, recuperar e consultar as informações relativas aos certificados, esse repositório na verdade é um banco de dados contendo todas as informações pertinentes. Elas também devem manter uma lista de certificados revogados, em que a publicação deve ocorrer periodicamente. (MONTEIRO, MIGNONI. 2007)

Os autores afirmam que para uma AC emitir certificados digitais, elas devem seguir claramente uma Declaração de Práticas de Certificação (DPC), essa DPC deve ser publicada publicamente para que todos tenham acesso e possam saber como foi emitido o certificado digital, porém cabe a AC implementar maiores medidas de segurança no seu parque tecnológico, ambiente físico e treinamento de

funcionários e colaboradores. Muitos fraudadores roubam informações pessoais de pessoas e empresas, com o intuito de falsificar documentos e, se passarem por alguém que não são com a finalidade de obter um certificado digital de forma fraudulenta. Portanto a maior obrigação relacionada a uma AC é a validação e verificação da identidade do titular do certificado digital, pois o mesmo deve conter informações confiáveis permitindo que a identidade de seu titular possa ser verificada.

Segundo a Cartilha do Certificado Digital (acesso em: 07/04/2015) as políticas adotadas por uma autoridade certificadora devem ser bem definidas para creditar maior credibilidade. Para que uma AC possa ser credenciada e fazer parte da ICP Brasil ela deve atender as exigências do comitê gestor que é responsável por especificar os procedimentos a serem adotados pelas ACs. As autoridades certificadoras passam por constantes fiscalizações, tanto de seus documentos quanto de suas instalações físicas e pessoas contratadas, a inconformidade nas fiscalizações podem levar uma AC ao descredenciamento, deixando de fazer parte da hierarquia ICP Brasil, que representa a garantia dos critérios estabelecidos sempre com a intenção de proteger as chaves privadas.

Fontes (2008) explica que para obter-se um certificado digital da cadeia ICP Brasil é necessária a validação presencial junto a uma autoridade certificadora vinculada, esse órgão é responsável pela confirmação dos dados a serem vinculados ao seu certificado digital.

A Cartilha de Segurança na Internet (2012) afirma que a AC também é responsável pela publicação na Lista de Certificados Revogados, que deve ser atualizada periodicamente e publicada como um arquivo eletrônico. O certificado digital de uma AC normalmente é emitido por outra AC, criando assim uma cadeia de certificados. A AC raiz é responsável por toda cadeia e possui um certificado autoassinado, que é aquele no qual dono e emissor é a mesma entidade.

Fontes (2006) explica que nos campos obrigatórios de dados de um certificado encontram-se os dados e assinatura da entidade responsável por sua emissão, permitindo assim que sua autenticidade e integridade sejam colocadas à

prova. A entidade responsável é uma Autoridade de Registro, ela é o principal componente de uma infraestrutura de chaves públicas, sendo a responsável pela emissão dos certificados digitais. Sendo a ICP Brasil a AC Raiz. Portanto fica a critério dos clientes escolherem em qual AC vão confiar para a emissão de seus respectivos certificados digitais.

2.2 TECNICAS UTILIZADAS PELOS ENGENHEIROS

Segundo Sales, Lima e Miranda em seu artigo Privacidade e Internet (acesso em: 09/05/2015), com o avanço da sociedade e consequentemente o avanço tecnológico houve maior popularização do acesso à rede, propiciando uma revolução tecnológica, e tal conceito de realidade incorporou uma nova visão ao nosso cotidiano até então desconhecida.

Por isso os autores afirmam que em decorrência dessa nova realidade é necessário observar as consequências oriundas que afetam diretamente a privacidade e intimidade do homem, que acaba por se tornar a única vítima relacionada a seu progresso.

> Só existe ma maneira de manter seguros os seus planos de produto: Ter uma força de trabalho treinada e consciente. Isso envolve o treinamento nas políticas e procedimentos, mas também – e provavelmente mais importante – um programa constante de conscientização. Algumas autoridades recomendam que 40% do orçamento geral para segurança da empresa seja aplicado no treinamento da conscientização. (MITNICK, SIMON 2003, p.195).

Peixoto (2006) explica que as empresas investem, cada vez mais, em seus parques tecnológicos, porém, em sua maior parte não realizam o mesmo investimento relacionado ao fator humano, principal vulnerabilidade explorada pelos engenheiros sociais. O principal foco de ataque dos engenheiros sociais está relacionado às grandes organizações, pois, segundo uma pesquisa realizada em 2002 pela revista norte americana *Information Security*, os investimentos relacionados a segurança da informação não acompanham o crescimento desestruturado das organizações. Infelizmente, o Brasil ainda não possui uma legislação específica relacionada a esse tipo de crime, portanto, as empresas necessitam implementar treinamentos constantes, além de elaborar um plano de contingência em caso de um possível ataque.

Afirma também que as técnicas da engenharia social consistem basicamente em obter informações privilegiadas, enganando usuários de sistemas e detentores de informações, entre as técnicas aplicadas pelos engenheiros sociais temos o uso de telefonemas, coleta de informações da internet, intranet, e-mail, pessoalmente, correspondência, coleta do lixo e surfar sobre ombros.

Para Rosa (acesso em: 09/05/2015), o principal ponto que a segurança da informação deve investir, está diretamente relacionado às pessoas. Para que toda a estrutura dentro de uma organização possa funcionar de forma eficaz, garantindo assim, a confidencialidade, a integridade e a disponibilidade, porém, é necessária também a conscientização dos usuários dentro da organização no que se refere a segurança das informações.

Como já citado no capítulo anterior Peixoto (2006) explica que o perfil do engenheiro social é sempre o de uma pessoa agradável, carismática, simpática e educada e, diversas pessoas já fizeram uso da engenharia social para obter as informações de que precisavam, existem diversas táticas e ferramentas utilizadas pelos engenheiros sociais para obter êxito em suas ações. A seguir algumas táticas mais frequentemente aplicadas pelos engenheiros sociais.

2.2.1 Análise do lixo

Segundo Mitnick e Simon (2003) o lixo é um grande meio de conseguir informações sigilosas de uma empresa, seja por listas desatualizadas de colaboradores, ou até mesmo manuais de equipamentos jogados fora, para uma pessoa qualquer isso não oferece risco algum, porém, nas mãos de um engenheiro social, isso se torna uma verdadeira arma.

Peixoto (2006) reforça a opinião de Mitinick e Simon ao dizer que documentos descartados no lixo podem conter informações cruciais de uma organização, e que engenheiros sociais habilidosos podem fazer uso da mesma.

Segundo Rafael (acesso em: 08/05/2015), poucas organizações tomam os cuidados necessários com o descarte de suas informações. O lixo é um dos meios mais ricos pelo qual um engenheiro social habilidoso pode conseguir informações

cruciais de uma organização. Portanto, todo cuidado é pouco relacionado ao descarte de documentos de uma empresa, existem diversos relatos relacionados ao uso dessa tática para obter informações importantes.

Um grande exemplo real de informações importantes de uma organização encontradas no lixo foi exibido em um documentário do Discovery Channel chamado Hackers anjos e Criminosos (2009), relata o ataque que Ian Murphy, o famoso capitão Zap realizou contra a empresa norte americana AT&T. Vasculhando o lixo da empresa, ele encontrava caixas e manuais descartados dos aparelhos implementados na organização, com esse tipo de informação, conseguia obter conhecimento das configurações aplicadas e, muitas das senhas padrões dos equipamentos, que sequer tinham sido alteradas. Em posse dessas informações invadiu os sistemas da AT&T e alterou os relógios dos sistemas da organização, assim conseguiu baixar os valores das ligações em horários de pico. Esse foi considerado o maior ataque de Hacker do mundo, tal feito só foi descoberto na emissão das faturas e, o famoso Capitão Zap já havia sumido, só foi capturado dezoito meses depois.

Para uma maior proteção nesse campo, o ideal seria o uso de um triturador e uma fragmentadora, para destruir totalmente todos os documentos, manuais e embalagens de equipamentos adquiridos. (ALVES, acesso em: 09/05/2015).

2.2.2 Internet e redes sociais

Peixoto (2006) explica que através de páginas, sites de relacionamentos dentre outros, os engenheiros sociais conseguem obter informações importantes de pessoas e organizações.

Esclarecendo e complementando a afirmação de Peixoto, Sales, Lima e Miranda explicam que a informação é um bem precioso e de grande valor, sendo um bem social, com o advento da internet nunca foi tão fácil ter acesso às informações em qualquer tempo e lugar.

Destacam os autores que em decorrência da tecnologia atual, a internet rompe barreiras relacionadas ao privado e público e, na maior parte do tempo, o limite relacionado à privacidade e publicidade acaba tornando-se uma linha tênue.

Sales Lima e Miranda (acesso em: 09/05/2015), explicam que diante da nossa realidade, informações pessoais circulam pela rede, seja através das práticas comerciais, ou através de sites de relacionamentos. Tal prática possui aspectos negativos, uma vez que pode propiciar a obtenção indevida de informações pessoais que podem ter por fim um uso fraudulento, ocasionando violação de privacidade e comercialização indevida das informações.

E ainda apresentam que tais práticas permitem que um tipo específico de coleta de informação seja amplamente utilizado, sendo ela a PII (*Personally Identifiable Information*), onde as informações coletadas são referentes à vida de pessoas, traçando um perfil completo com os dados coletados. Esses dados adquiridos em meio eletrônico se referem a uma pessoa de carne e osso, ou seja, a alguém que realmente existe, que possui identificação, um endereço, uma vida.

Sales Lima e Miranda (acesso em: 09/05/2015), salientam que diversas empresas como operadoras de cartão de crédito, operadoras de telefonia celular, hospitais, bancos dentre outros, mantém um registro com informações relevantes de seus usuários, que nas mãos de engenheiros sociais habilidosos, podem se tornar uma ameaça.

Um bom exemplo da aplicação desse tipo de tática da engenharia social é um caso recente, a revista Veja digital relatou que a casa de uma casal de engenheiros foi invadida por uma dupla de assaltantes que procuravam por equipamentos eletrônicos recentemente adquiridos pelo casal, eles tinham acesso a esse tipo de informação, pois o filho do casal havia postado fotos nas redes sociais informando a aquisição dos aparelhos eletrônicos de última geração. (VEJA, acesso em: 24/05/2015)

Na Constituição Federal do Brasil (2008), o artigo 5º, inciso X, estabelece que a privacidade é um direito básico.

> Art. 5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e a propriedade, nos termos seguintes (...)
>
> X- são invioláveis a intimidade, à vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (...) (CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Acesso em: 24/05/2015)

Sales Lima e Miranda, afirmam que a internet pode ser classificada como um meio de comunicação em massa. Portanto, os conceitos de privacidade e intimidade podem ser perfeitamente aplicados dentro do conceito de internet. Dessa forma qualquer violação relacionada à honra, à intimidade, à vida privada entre outros, constitui crime contra a privacidade e intimidade.

2.2.3 Contato telefônico

Rosa (acesso em: 09/05/2015) explica que contatos telefônicos são uns meio muito utilizados no contexto de engenharia social, muitas vezes passando-se por alguém dentro da organização, como alguém da equipe de TI ou de suporte para conseguir informações privilegiadas.

No documentário exibido pela *Discovery Channel Hackers* Anjos e Criminosos um profissional que atende pelo nome de Bryan Holyfield, atua como um *hacker* ético, ele e sua equipe são conhecidos como time dos tigres é pagos por grandes organizações para invadirem suas redes, para poderem encontrar as vulnerabilidades do sistema, evitando que engenheiros sociais façam uso dessas vulnerabilidades. A maior tática utilizada por Bryan é justamente o contato telefônico, normalmente se passa por alguém do suporte ou da equipe de TI, para obter informações privilegiadas das organizações. Para isso faz uso da simpatia, e solicita a senha, alegando que é apenas um teste do sistema, de forma surpreendente sempre obtêm resultados com essa técnica.

Rafael (acesso em: 08/05/2015), explica que normalmente antes dessa etapa, o engenheiro social já conseguiu obter informações importantes através da coleta do lixo e da internet e redes sociais, portanto, nessa etapa normalmente está familiarizado com os nomes e, com a linguagem utilizada dentro da organização.

2.2.4 Abordagem pessoal

Peixoto (2006) explica que nesse tipo de tática, o engenheiro social utiliza o poder de persuasão, usando os conhecimentos adquiridos e a simpatia para se passar por alguém que não è, esse tipo de ataque é mais raro, uma vez que o engenheiro social precisa de informações importantes do território que vai atacar para alcançar esse fim.

Rafael (acesso em: 08/05/2015), acrescenta que embora seja uma técnica arriscada, muitos engenheiros sociais fizeram e fazem uso dessa técnica até hoje. Normalmente nesse tipo de técnica, o engenheiro social procura se passar por um fornecedor da empresa, amigo ou parente do proprietário; fazendo uso da simpatia e da persuasão, por falta de treinamento de muitos funcionários, consegue adentrar as dependências da organização, tendo acesso ao *datacenter,* onde provavelmente, vai conseguir as informações das quais necessita.

2.2.5 Phishing

"*Phishing, phishing-scam ou phishing/scam*, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p. 9).

A Cartilha de Segurança para Internet (2012) explica que diante da dificuldade em obter acesso aos dados armazenados pelos bancos, muitos engenheiros sociais optaram por atacar diretamente os usuários desses sistemas. Através do uso de técnicas de engenharia social, os golpistas procuram persuadir e enganar suas vítimas, orientado as mesmas a executarem softwares maliciosos, ou acessar páginas falsas. Em posse dos dados das vítimas, eles têm acesso as suas informações, abrindo contas bancárias, acessando contas já existentes, abrindo firmas fantasmas, emitindo certificados digitais em prejuízo de um terceiro, entre outras atividades maliciosas.

Rafael (acesso em: 08/05/2015) reforça a afirmação, alegando que essa é uma das táticas mais comuns aplicadas dentro do contexto da engenharia social,

normalmente o objetivo desse tipo de golpe é conseguir informações básicas, como números de documentos, de cartões de créditos, conta corrente entre outros.

Esclarece que o intuito nesse tipo de ataque normalmente é obter acesso ao dinheiro que consta nas contas desses usuários explorando a confiança dos mesmos. Como os sistemas bancários são seguros, acabam dificultando a obtenção de informações. Os engenheiros sociais aplicam o golpe diretamente nos clientes dos bancos, que normalmente estão menos preparados a esse tipo de ataque. Nesse tipo de golpe criam uma página semelhante a do banco original, enviam o link por e-mail e solicitam que o usuário se cadastre, porém quando o usuário insere suas informações e senhas, na verdade estão acessando uma página *fake*, ao invés do banco, são os criminosos que estão fazendo uso dessas informações privilegiadas.

O pesquisador brasileiro Assolini (acesso em: 26/06/2015) explica que um novo tipo de fraude utilizando *phishing* vem sendo utilizado, ele identificou em tentativas de fraude recentes um novo vírus capaz de falsificar o certificado digital *Secure Sockets Layer* (SSL), que são os certificados digitais utilizados para sites de internet. Quando se acessa uma página protegida por um certificado digital SSL, um ícone com um cadeado aparece comprovando que essa página é segura, e o certificado digital é válido e emitido por uma Autoridade Certificadora. Porém o vírus recentemente desenvolvido é capaz de burlar a segurança dos navegadores, como é impossível duplicar m certificado digital já existente, o vírus que ainda não possui um nome “instala uma autoridade certificadora”, portanto nesse processo, o navegador confirma a segurança do site.

Para se proteger desse tipo de tática utilizada pelos engenheiros sociais, o pesquisador aconselha que seja solicitada as informações do certificado SSL quando o navegador acessar uma página com cadeado, lembrando que essa vulnerabilidade não é dos protocolos de segurança do cadeado que representam os certificados digitais, mas sim do vírus instalado no computador.

2.2.6 Falhas Humanas

> Os engenheiros sociais habilidosos são adeptos do desenvolvimento de um truque que estimula emoções tais como medo, agitação, ou culpa. Eles fazem isso usando os gatilhos psicológicos – os mecanismos automáticos que levam as pessoas a responderem as solicitações sem uma análise cuidadosa das informações disponíveis. (MITNICK, SIMON, 2003, p.85).

Quando se analisa o contexto de segurança da informação, a primeira ideia que surge, é a de correção dos erros computacionais, logo vem a mente a implementação de *firewalls*, *anti spywares*, tudo com o intuito de bloquear e remover *softwares* maliciosos, a implementação de todas as barreiras de segurança possíveis, porém com uma simples falha de um operador, todo o sistema pode ser comprometido. (BRAGA, 2010).

O autor afirma que o apelo sentimental ainda é uma forte tática utilizada pelos engenheiros sociais para obterem acesso as informações das quais necessitam.

Rosa (acesso em: 08/05/2015), explica que como já afirmado e apresentado no capítulo anterior, não se pode negar que independente de todos os recursos aplicados e voltados para a segurança, o homem continua sendo o elo mais fraco nesse quesito, principalmente, no que concerne a engenharia social.

Segundo Peixoto (2006), dentro do conceito de engenharia social, compreende-se a inaptidão que diversas pessoas possuem na falha de proteger informações importantes, ou na falta de conhecimento da importância que essa informação possui. Abordar-se á alguns conceitos do comportamento do ser humano que tornam possíveis as ações dos engenheiros sociais:

- Vaidade pessoal e profissional: De modo geral são receptivas a elogios e agrados, portanto aceitam facilmente argumentos favoráveis em benefício próprio ou coletivo.

- Autoconfiança: Se comunicam de forma individual e coletiva objetivando sucesso, de forma coletiva ou individual, com o intuito de criar uma comunicação favorável para uma organização ou para algum indivíduo.

- Formação profissional: Busca, através de sua formação profissional, o reconhecimento pessoal e profissional sempre como um primeiro objetivo.

- Vontade de ser útil: De modo geral, buscam ser úteis e agradar aos outros, para se destacar e crescer profissionalmente.

- Busca por novas amizades: Para agradar aos outros, procura ser útil, buscando aprovação e elogio de outras pessoas.

- Propagação de responsabilidade: Na maioria dos casos, não se considera o único responsável pelas atividades desempenhadas.

- Persuasão: É basicamente a capacidade de manipular pessoas para obter as informações das quais necessita. Tal tática só é possível por que o ser humano possui um comportamento manipulável.

É importante lembrar que a engenharia social não está ligada somente a área de tecnologia da informação, ela é, basicamente, uma ferramenta pela qual o ser humano busca encontrar vulnerabilidades para atingir o seu propósito. (PEIXOTO, 2006)

Popper e Brignoli (acesso em: 09/05/2015) explicam que, analisando de forma minuciosa, pode-se notar que em sua maioria, as grandes empresas já sofreram algum ataque de engenharia social. Quem nunca se viu em uma conversa e, no decorrer do assunto, notou que entregou certas informações somente através de um bate papo, isso quando percebe que entregou as informações.

Os autores afirmam que em grandes empresas, organizações militares, hospitais, instituições financeiras entre outros a situação não é diferente, porém nesse caso pessoas mais habilidosas estão envolvidas, ou seja, os famosos engenheiros sociais.

Em uma tentativa de tornar as emissões de certificados digitais mais seguros, o ITI está implementando uma nova forma de autenticação para a emissão de

certificados digitais, sendo ela o uso da biometria. Com essa nova técnica pretende-se coagir os fraudadores, e dificultar a emissão de certificados digitais fraudulentos. (ITI, acesso em 24/05/2015).

Diante do conteúdo abordado neste capítulo, pode-se notar a grande aplicabilidade que os certificados digitais possuem, permitindo inúmeras possibilidades de autenticação com seu uso. A ICP Brasil disponibiliza a toda hierarquia vinculada a ela, uma DPC (Declaração de Práticas de Certificação) que deve ser seguida para garantir maior segurança ao ambiente físico e lógico, porém, cabe as Autoridades Certificadoras implementar maiores medidas de segurança com a finalidade de tornar a emissão segura contra fraudes. Portanto, um sistema de autenticação desse porte desperta o interesse de fraudadores, que utilizam as técnicas da engenharia social para coletarem informações, falsificando assim documentos com o intuito de se passarem por outra pessoa, e obter um certificado digital de forma fraudulenta em prejuízo de outra pessoa.

3 CONSIDERAÇÕES FINAIS

A partir da apresentação e análise das informações coletadas, podemos notar que segurança da informação é um requisito básico a ser implantado dentro das organizações, uma vez que a informação é o principal ativo de uma empresa. Sendo assim, a segurança da informação consiste basicamente em implementar requisitos de segurança e políticas a serem seguidas, com o intuito de proteger a informação contra fraude e uso ilícito.

Outra questão importante diz respeito ao uso da engenharia social, para obter informações importantes dentro de uma organização. Os famosos engenheiros sociais, nem sempre utilizam recursos tecnológicos para acessarem ilicitamente as informações das quais necessitam. Em sua maioria, atacam a maior vulnerabilidade de uma organização, o fator humano.

É importante salientar que com a evolução tecnológica ocorrida através dos anos, houve grande evolução nesse campo, como as transações online aumentaram através dos anos, foi necessário desenvolver um método de se autenticar no meio digital, garantindo assim a confidencialidade, integridade e, não repúdio das informações prestadas. Dessa forma surgiram os certificados digitais, que oferecem a possibilidade de se autenticar no meio digital, garantindo maior confiabilidade nas ações efetuadas através do meio digital.

Obviamente, que um recurso que possibilita inúmeras vantagens no meio digital, despertou o interesse de fraudadores, que através do uso da tecnologia e da engenharia social, tentam obter um certificado digital de forma ilícita em prejuízo de terceiros. Para tanto, eles fazem uso de algumas técnicas da engenharia social, sendo elas tecnológicas ou não, que possibilitam o roubo de informações pertinentes a uma organização.

Para garantir maior confiabilidade na emissão de certificados digitais, e minimizar possíveis fraudes, o Governo Federal implementou uma hierarquia vinculada a ICP Brasil, sendo a AC de primeiro nível o ITI. O propósito dessa

hierarquia é implementar políticas de segurança para tornar as emissões de certificados digitais mais segura.

Atrelado às questões acima citadas, um exemplo claro de tentativa de fraude de certificado digital em prejuízo de terceiros documentado pelo site Mac Magazine (acesso em: 24/05/2015), foi o ataque aos sistemas de uma empresa afiliada a AC Comodo que teve seus sistemas invadidos por *hackers* habilidosos, que conseguiram através do uso de meios computacionais e engenharia social, obter usuário e senha do sistema de emissão de certificados. Através desse ataque nove certificados fraudulentos do tipo *Secure Socket Layer* (SSL), que são basicamente certificados digitais utilizados em sites de internet foram emitidos, sendo eles de grandes empresas, tais como, Skype, Google, Mozila e, Yahoo. O maior problema encontrado nessa emissão fraudulenta, é que mesmo após a revogação desses certificados, muitos usuários de internet podem visualizar os sites como válidos, pois nem todos os usuários utilizam navegadores que reconhecem automaticamente a validade dos certificados digitais.

Através do ataque realizado aos sistemas da Comodo é possível observar a seriedade que o requisito segurança da informação possui dentro de uma organização, e como *hackers* habilidosos conseguem acessar as informações das quais necessitam, utilizando-se de conhecimentos computacionais e técnicas engenharia social. Mesmo com todas as políticas implementadas pelo ITI, é possível observar que os sistemas ainda são passíveis de ataques e falhas. É importante observar a seriedade desse tipo de ataque e emissão fraudulenta que, possibilita aos atacantes criarem páginas falsas, como as de *phishing,* com a capacidade de se passarem por alguém que não são e, obterem informações sigilosas de seus usuários.

Na tentativa de tornar os sistemas relacionados a emissão de certificado digital mais seguros, o ITI pretende adotar a biometria como requisito básico na emissão de certificados digitais.

Infelizmente, ao analisarmos o objeto de estudo, é possível observar que ainda é necessário evoluir muito nesse campo, pois *hackers* sempre vão procurar por brechas nos sistemas, seja pelo meio computacional ou não.

Podemos observar que existem diversas técnicas utilizadas pela engenharia social com a finalidade de obter informações privilegiadas de uma organização. Tais técnicas possibilitam aos engenheiros sociais alcançarem sua finalidade.

Apesar de todas as políticas padrões elaboradas pelo ITI e relacionadas a toda hierarquia vinculada a ICP Brasil, o usuário não está totalmente protegido, pois hackers habilidosos quebram qualquer codificação e, apesar de todas as políticas implementadas, e todos os recursos de segurança da informação ativos, não existe sistemas 100% seguros, pois através do uso da engenharia social, fraudadores sempre vão tentar obter informações através de meios ilícitos.

De forma geral, o certificado digital é um meio de autenticação seguro, que possibilita a seu usuário, autenticar-se no meio computacional, garantindo autenticidade, integridade e perenidade de conteúdo. Porém, torna-se necessário a elaboração de novas políticas que tornem as emissões mais seguras.

Sugere-se que um novo projeto relacionado a políticas a serem implementadas para aumentar a segurança na emissão de certificados digitais seja proposta, com o intuito de tornar esse tipo de ação cada vez mais segura.

REFERÊNCIAS

ARANHA, Anna Carolina. **A sociedade e a segurança da informação.** Disponível em: https://technet.microsoft.com/pt-br/library/cc668426. Acesso em: 01 mar. 2015. 15h12.

ASSOLONI, Fábio. **Vírus Falsifica o Cadeado de Certificação Digital.** Disponível em: http://www.tecmundo.com.br/virus/6913-virus-falsifica-o-cadeado-de-certifica cao- digital.htm. Acesso em: 31 maio 2015. 09h32.

ALVES, Cássio Bastos. **Segurança da Informação VS. Engenharia Social**: Como se Proteger para não ser mais uma Vítima. Disponível em: Alveshttp:// monografias.brasilescola.com/computacao/seguranca-informacao-vs engenharia-social-como-se-proteger.htm. Acesso em: 11 maio 2015. 14h10.

BRAGA, Pedro Henrique da Costa. **Técnicas de Engenharia Social**. Disponível em: http://gris.dcc.ufrj.br/documentos/artigos/engenharia-social. Acesso em: 08 maio 2015. 12h31

CARTILHA DO CERTIFICADO DIGITAL. Disponível em: https://www.oficioeletronico. com.br/Downloads/CartilhaCertificacaoDigital.pdf. Acesso em: 24 maio 2015.

CARTILHA DE SEGURANÇA PARA INTERNET. 2012. Disponível em: http://cartilha. cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 24 maio 2015. p.5-13, 67-72.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. **Artigo 5° Inciso X.** Disponível em: http://www.planalto.gov.br/ccivil03/constituicao/ constituicao. htm. Acesso em: 24 maio 2015. 23h54.

DENZIN, N. e LINCOLN, Y. **Planejamento da pesquisa qualitativa** – teorias e abordagens. Porto Alegre: Artmed. 2006. p. 2.

DISCOVERY CHANNEL. **Hackers Anjos e Criminosos**. 2009. Disponível em: https://www.youtube.com/watch?v=vLulG30EM9c. Acesso em: 03 maio 2015.

FACHIN, O. **Fundamentos de Metodologia**. São Paulo: Saraiva, Brasil. 2006. p.32

FERREIRA, F. ARAÚJO, M. **Política de segurança da informação**: guia prático para elaboração e implementação. Rio de Janeiro: Moderna. 2006. p. 9-28; 76-81; 85; 9-28; 92-102.

FONTES. E. **Praticando a Segurança da Informação**: orientações e práticas alinhadas com as normas. Rio de Janeiro: Brasport. 2008. p.109-117; 119-134; 139-149.

_____. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Saraiva. 2006. p. 1-3; 11-13; 20-26; 34-39; 45-54; 59-60; 65-68; 74-75; 81-92; 98-104; 120-122.

GOUVÊA, S. **O Direito na Era Digital**: crimes praticados por meio da informática. Rio de Janeiro: Mauad. 1997. Disponível em: https://books.google.com.br/books?id=3vzmW3DtAuQC&pg=PP4&lpg=PP4&dq=GOUV%C3%8AA,+E.+O+Direito+na+Era+Digital&source=bl&ots=TErCOnUivx&sig=p1tPx0qSYrnLntxvGgxWpR35vgg&hl=pt-BR&sa=X&ei=E_huVYmwDMe5ggT4_YKQCQ&ved=0CCEQ6AEwAA #v=onepage&q=GOUV%C3%8AA%2C%20E.%20O%20Direito%20na%20Era%20Digital&f=false. Acesso em: 27 nov. 2014. 10h01.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Combate as Fraudes:** Solução Biométrica é apresentada ao ITI. Disponível em: http://www.iti.gov.br/noticias/indice-de-noticias/4790-combate-as-fraudes-solucao-biometrica-e-apresentada-ao-iti. Acesso em: 23 maio 2015. 21h17.

LUCCA, Newton. FILHO, Adalberto Simão. **Direito & internet**: aspectos jurídicos relevantes. São Paulo: Quartier Latim. 2005. p. 411-420; 450-456.

MACMAGAZINE. **Roubos de Certificados Digitais pode Expor Usuários a Fraudes Online**. Disponível em: https://macmagazine.com.br/2011/03/25/roubo-de-certificados-digitais-pode-expor-usuarios-a-fraudes-online/. Acesso em: 23 maio 2015. 14h05.

MARCONI, M. LAKATOS, E. **Técnicas de Pesquisa**. São Paulo: Atlas, Brasil. 2011. p. 6, p.12.

MITNICK, K. SIMON, W. **A Arte de Enganar:** Ataques de Hackers Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Brasil. 2003. P.3-24; p.85; p.195-205.

MONTEIRO, E. MIGNONI, M. **Certificados Digitais:** Conceitos e Práticas. Rio de Janeiro: Brasport, Brasil. 2007. p. 5-70.

PEIXOTO, M. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, Brasil. 2006. p.3-49.

POPPER, Marcos Antonio; Brignoli, Juliano Tonizetti. **Engenharia Social:** Um Perigo Eminente. Disponível em: http://www.posuniasselvi.com.br/artigos/rev03-05.pdf. Acesso em: 09 maio 2015. 18:15.

PRADO, E. SOUZA, C. **Fundamentos de Sistemas de Informação.** Rio de Janeiro: Elsevier. Brasil. 2014. p.93-107.

RAFAEL, Gustavo de Castro. **Engenharia Social**: As técnicas de Ataque mais Utilizadas. Disponível em: http://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/. Acesso em: 09 maio 2015. 13h23.

LENNERT, Luiz Sérgio e OLIVEIRA, Marcos Altemari de. Engenharia Social: Uma ameaça Fraudulenta Crescente. (2011). **Revista Gestão de Riscos**. Disponível em: http://www.brasiliano.com.br/wp/wp-content/uploads/2013/03/edicao_64.pdf. Acesso em: 02 jun. 2015. 17h00.

REVISTA VEJA. **Informações em Rede social Estimularam Roubo em São Paulo**. Disponível em: http://veja.abril.com.br/noticia/brasil/informacoes-em-rede-social-estimularam-roubo-em-sp/. Acesso em: 24 maio 2015. 22h15.

ROSA, Aguinaldo Fernandes. **Engenharia social:** Explorando o elo mais fraco. Disponível em: http://securityone.com.br/artigos/resenha_engenharia_social.pdf. Acesso em: 08 maio 2015. 16h23.

SALES, Fábio Augusto Cornazzani; LIMA Gisele Truzzi de e MIRANDA, Rodrigo Barros de MIRANDA. **Privacidade e internet.** Disponível em: http://www. truzzi.com.br/pdf/artigo-privacidade-internet-gisele-truzzi-fabio-augusto-cornazzani-sales-rodrigo-barros-de-miranda.pdf. Acesso em: 10 maio 2015. 13h45.

SÊMOLA, M. **Gestão da Segurança da Informação**: uma visão executiva. Rio de Janeiro: Campus. 2003. p.1-25; 43-54; 82-115.

SINDICATO DAS EMPRESAS DE SEGUROS, RESSEGUROS E CAPITALIZAÇÃO (28/11/2014). **Alertas às ARS:** tentativas de fraude na emissão de certificado digital. Disponível em: http://www.sindsegsp.org.br/site/noticia-texto.aspx?id=16725. Acesso em: 23 fev. 2015. 18h10.