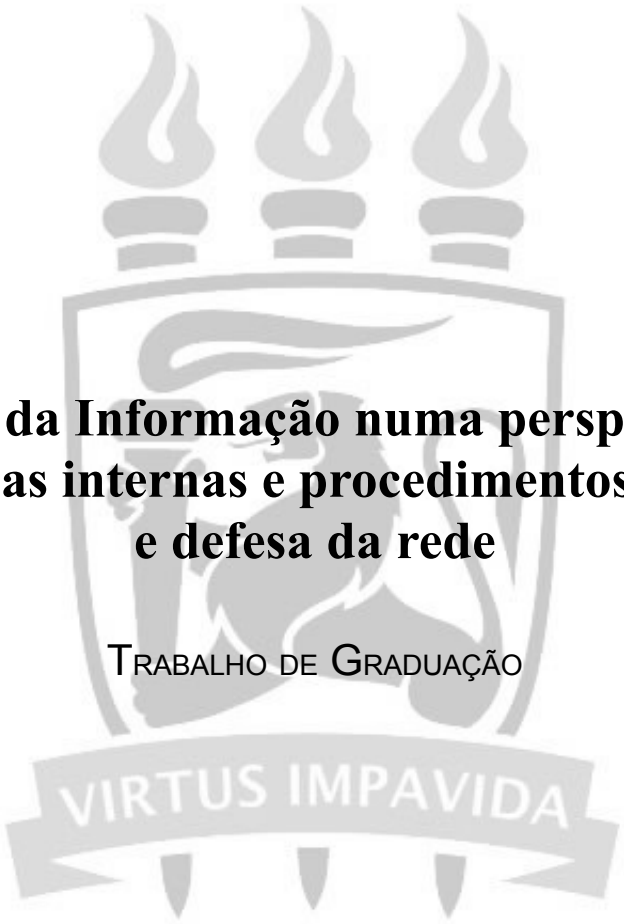
Universidade Federal de Pernambuco
Graduação em Ciência da Computação
Centro de Informática



Segurança da Informação numa perspectiva mais humana. Falhas internas e procedimentos de prevenção e defesa da rede

Trabalho de Graduação

Aluno: Felipe Ribeiro Machado (frm@cin.ufpe.br)

Orientador: Ruy José Guerra Barretto de Queiroz (ruy@cin.ufpe.br)

Recife, 2009

UNIVERSIDADE FEDERAL DE PERNAMBUCO
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO
CENTRO DE INFORMÁTICA

Segurança da Informação numa perspectiva mais humana. Falhas internas e procedimentos de prevenção e defesa da rede

TRABALHO DE GRADUAÇÃO

Monografia apresentada ao Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Ciências da Computação.

Aluno: Felipe Ribeiro Machado

Orientador: Ruy José Guerra Barretto de Queiroz

Recife, 2009

Aos meus familiares.

Agradecimentos

Agradeço a Deus, a Santa Luzia, a Nossa Senhora, ao meu Anjo da Guarda e ao Divino Espírito Santo por terem me guiado e demonstrado o melhor caminho a ser seguido em direção às vitórias ou a outros caminhos melhores. A minha mãe Maria Fernanda, avó Milene Alves, e ao meu avô Paulo de Souza Ribeiro, meus irmãos Paulo Ribeiro e Reivel Júnior por terem me oferecido totais condições de trabalho e terem me garantido conforto e me deixado com uma única preocupação: desenvolver os estudos. Agradeço aos colegas da faculdade, Thiago Pacheco, Leonardo Luiz, Josinaldo Júnior e Glérter Alcântara Sabiá que me ajudaram no sucesso, ora compreendendo algumas limitações minhas, ora apoiando decisões e me dando apoio sabendo de minhas vantagens que cobririam as desvantagens nos nossos demorados e duros projetos. Aos meus familiares em geral que tanto vibraram e me apoiaram. Aos meus amigos que tanto acompanharam e me aconselharam nos momentos mais difíceis. Ao meu orientado Ruy Guerra que me acolheu nesse projeto e me fez acreditar na importância e qualidade que este trabalho estava sendo desenvolvido.

Resumo

Este trabalho falará da ocorrência de falhas humanas no processo de cuidado com informações empresariais digitalizadas. Será destacada a exposição dos dados na Internet, o risco, e de diversas outras ameaças além de citar ocorrências reais e perdas percebidas causadas por estes diversos tipos de ataques. Serão comentadas fragilidades humanas no processo de segurança e sobre até que ponto é importante a conscientização das pessoas quando nos referimos a segurança da informação. Procedimentos de defesa serão frisados tanto no ponto de vista tecnológico quanto humano bem como a busca pela conscientização das pessoas que compõem a instituição. Seriam as pessoas da instituição importantes na defesa de um sistema? Haveria tecnologia e processos que supririam o capital humano na proteção dos dados?

Palavras-chaves: Falhas humanas, risco, conscientização, proteção dos dados.

ABSTRACT

This work will speak about the occurrence of human error in the care of digital business information. Will be highlighted, the exposure of data on the Internet, the risk, and various other threats besides cite actual events and perceived losses caused by these different types of attacks. Will be discussed weaknesses in the process of human security and on how important it is the awareness of people when we refer to information security. Procedures for the defense will be emphasized both at the point of view of technology as well as the human quest for awareness of the people who make up the institution. People would be important in defending the institution of a system? There would be technology and processes to meet the human capital in data protection?

Keyword: *Human error, risk, awareness, data protection*

Sumário

1 – Introdução.....1

1.1 – Informação, sua importância e exposição.....1

1.2 – A tecnologia por si só já não seria suficiente? 3

1.2 – Trabalho realizado.....4

1.3 – Organização do documento.....4

2 – Ataques a sistemas e perdas reconhecidas.....5

2.1 – Aumento de Produção de Pragas Eletrônicas e Ataques Realizados.....6

2.2 – Diferentes tipos de ataques.....8

2.2 – Exemplos reais de ataques e perdas reconhecidas.....12

2.3 – Fragilidade humana referente às falhas.....14

3 – Falhas humanas percebidas.....16

3.1 - Falta de treinamento ao recurso humano.....16

3.2 - Falta de investimento humano/tecnológico.....17

3.3 - Falhas humanas.....18

3.4 - Fragilidade frente engenharia social.....20

3.5 - Más-intenções.....22

3.6 - Ignorância dos usuários.....23

3.7 - Falha dos implementadores do software.....25

4 - Procedimentos de defesa.....29

4.1 - Organização da Segurança da Informação.....30

4.2 - Política de Segurança da Informação.....34

4.3 – Treinamento/educação ao recurso humano.....35

4.4 – Procedimentos básicos preventivos de defesa.....41

4.5 - Segurança Física.....43

5 – Conclusão e Trabalho Futuro.....46

6 – Referências Bibliográficas.....48

APÊNDICE A – Glossário.....53

Índice de figuras

Ilustração 1: Total de Incidentes Reportados ao CERT.br por Ano.....7

Ilustração 2: Phishing simulando correspondência da Receita Federal.....11

Ilustração 3: Problemas que geraram perdas financeiras.....12

Ilustração 4: Linguagens de programação mais inseguras – TIOBE Software.....27

Ilustração 5: Aprendizagem contínua - Maconachy, Schou, Ragsdale e Welch.....37

1 – Introdução

Com a expansão da tecnologia e massificação quanto ao seu uso, as informações digitalizadas passaram a substituir os papéis abarrotados de escritas manuais ou datilografadas. Estas formas não digitalizadas de armazenagem eram os meios possíveis e mais acessíveis para viabilizar o tratamento de informações. Estas possuíam as mais diversas importâncias segundo critério de cada usuário ou de cada sistema de informação que as utilizassem. Os cuidados que eram exigidos no tratamento dos dados foram cada vez mais necessários tendo em vista que, acompanhando o crescimento da tecnologia, ataques com o intuito de obter informação desses sistemas de forma ilegal ou simplesmente corromper os dados eram realizados com as mais diversas finalidades ilícitas – desejo por fama sua (estimulando a publicidade quanto sua capacidade de invadir "qualquer" sistema) e de seu programa, finalidade de roubo de dados bancários, roubo de dados pessoais visando desvio de dinheiro ou aproveitamemto de compras *on-line* dentre tantos outros motivos.

Antes de quaisquer análises quanto a implementação de sofwares ou processos de defesa, faz-se necessária uma análise das pessoas que das tecnologias corporativas farão uso ou serão responsáveis por elas. Deve-se também haver um entendimento referente ao grau de importância de uma informação pessoal ou corporativa e dos prejuízo possíveis num caso de falhas que poderiam ser facilmente evitadas bastando apenas uma educação de alguns funcionários e usuários de uma empresa.

O trabalho destacará a importância da informação e a existência do risco dela pelos mais diversos motivos, assim como destacaremos sua natural exposição na Internet ou redes internas. Serão percebidos destaques sobre os diversos crimes virtuais possíveis e formas de ataque utilizadas sendo buscadas exemplificações sobre as ocorrências e perdas ocasionadas. Um foco maior será dado referente as pessoas que desta instituição façam parte percebendo todas elas como responsáveis pela segurança da informação cujas suas garantias de qualidade de fato serão muito além de restrições ao uso da tecnologia.

1.1 – Informação, sua importância e exposição

Atualmente a humanidade convive com uma realidade cuja possibilidade de evitá-la é descartável quando se fala em tecnologia: a informação digital. Desde simples computadores pessoais até empresas de quaisquer portes precisam armazenar dados – em geral, todo sistema ou máquina costuma guardar dados simples e corriqueiros sem maiores importâncias ou até com os maiores e mais diversos valoramentos. Nesses valores não são reconhecidos apenas os econômicos e estratégicos-empresariais. Informações mais simples como fotografias familiares ou de momentos da vida, músicas, textos marcantes, cartas ou algumas outras formas de dados que, apesar do baixo valor econômico para a maioria das pessoas, representam um bem insubstituível para aquele usuário – ou seja, para este(s) usuário(s), não há comparação quanto a uma outra espécie, qualidade e quantidade capaz de substituir este dado. Logo são percebidas as diversas formas de importância que uma informação possui. Num âmbito mais geral e visado por este trabalho, as informações, avaliadas segundo um critério corporativo, possuem, de início, um valor econômico agregado a outro valor estratégico, vital para o funcionamento e crescimento de uma instituição.

Importância da informação por si só já exigiria um cuidado sobre ela, tanto no aspecto de ser prejudicada num âmbito acidental - por exemplo, quebra de um disco rígido -, como quanto acidentes pré-meditado - um ataque por um vírus ou cracker que desejaria inutilizar aqueles específicos dados. Numa empresa, as informações constituem o bem de maior valor delas. Balloni diz que atualmente a informação é de valor altamente significativo e pode representar grande poder para quem a possui, seja pessoa, seja a empresa. A informação apresenta-se como recurso estratégico sob a ótica da vantagem competitiva. Possui valor, pois está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos financeiros, tecnologias e etc. [1]

Vale salientar também que a grande maioria destas informações essencias necessitam ser digitalizadas. É bom lembrar que existe a importância e agilidade conquistada pelo homem quando necessário o confronto da manipulação manual versus um controle informatizado de dados, torna-se praticamente obrigatório o uso de informações digitalizadas como a forma de manipulação efetiva e qualificada de fato dos dados. Consequentemente de nada adiantaria fugir da informação digital quando os ganhos resultantes desta são consideravelmente elevados e as despesas associadas ao menor tempo gasto na sua manipulação proporcionam um aumento significativo nos balanços financeiros empresariais por exemplo. Resultado: digitalizar informação é necessário e instrínseco ao acompanhamento dos processos comerciais na atualidade. Surge então o questionamento sobre a constante exposição que esta mesma digitalização proporciona junto a essa digitalização de dados – ou seja, informações importantes e sensíveis tendem a estar nesse conjunto de bits.

Tendo em vista então a importância da informação nos seus mais diversos meios, é

percebido que, mesmo que um aparente cuidado com estas informações não sejam necessários, a ocorrência de alguma perda de tais informações acarretará um considerável prejuízo percebido a curto, médio ou longo prazo.

Vale salientar finalmente a existência da *Internet* e o considerável número de informações que foram agregadas aos dados anteriores. À partir de então, é importante frisar os ganhos com a pesquisa de informação que irão culminar num "canal" aberto com a Rede Mundial de Computadores – não descartando pois uma forma de infecção do sistema pelas diversas pragas virtuais que pela *Internet* circulam.

1.2 – A tecnologia por si só já não seria suficiente?

Visando o processo de Segurança da Informação, é necessário considerar a existência de uma cadeia baseada na segurança cuja formação dela depende de três elos: tecnologias, processos e pessoas.

Frente a exposição constante das informações e conhecendo haver na tecnologia grande quantidade – e até boa qualidade – de programas cujo propósito é "impedir" o ataque de pragas virtuais, muitos entendem ser dispensável a influência humana no processo. Porém quando analisados os maiores causadores de falhas de segurança, são vistas as pessoas como os maiores responsáveis por incidentes representando aproximadamente 24% das ocorrências. [2]

Grande parte dos incidentes conta com participação humana, diretamente ou indiretamente, intencionalmente ou não. De início as pessoas costumam confundir a proteção das informações da empresa com a simples proteção da máquina. As atitudes em si, costumam ser deixadas num segundo plano.

Mais explicadas e exemplificadas posteriormente, falhas simples, como clicar em links suspeitos, escrever senhas em bilhetes colados à máquinas, sucumbir a um pedido mais gentil de informações sobre acesso estratégicos ou não instalar um patch de atualização de programa aplicativo ou Sistema Operacional alegando que "deixará mais lento o computador", são algumas das formas de caracterizar a falha humana. Estas mesmas pessoas que falham são as que utilizam os recursos tecnológicos. E esta tecnologia, sem correta utilização, pouco servirá com tamanhas brechas causadas pela falha humana.

1.2 – Trabalho realizado

O trabalho buscará uma explanação quanto a exposição da informação aos diversos riscos virtuais. Focará no aspecto humano da segurança mapeando as diversas formas de falha e medidas que deveriam ser utilizadas numa instituição para um melhoramento da defesa contra os crimes virtuais. Serão buscados exemplos comprovando as ideias e argumentos além da valorização do aspecto humano na defesa do sistema.

1.3 – Organização do documento

Este documento estará organizado segundo os seguintes critérios:

- [Capítulo 1] Introdução do trabalho onde é exposta a importância da informação bem como das pessoas da instituição.
- [Capítulo 2] Serão demonstradas ocorrências de ataques, os diversos meios que eles podem se manifestar, bem como o aumento destes ataques ocasionados pelas mais diversas formas além de algumas perdas básicas estimadas – importante frisar que outros ainda podem existir além dos analisados, entretanto os principais, os basilares, serão os destacados. Serão também demonstradas algumas falhas havendo principalmente um foco quando estas forem ocasionadas por falhas considerando-se à partir de uma visão do capital humano presente a corporação.
- [Capítulo 3] Análise de falhas ocorridas no foco humano. Deve-se frisar que as falhas serão baseadas em faltas cometidas tanto por usuários finais como pelos próprios implementadores e projetistas do sistema.
- [Capítulo 4] Procedimentos de defesa serão propostos para realização dos diversos exemplos comentados nesse trabalho além de outros a serem acrescentados.
- [Capítulo 5] Conclusão e proposta de trabalho futuro em que se propõe um processo inicial numa viabilização na defesa de um sistema.

2 – Ataques a sistemas e perdas reconhecidas

Quando ocorrem ataques a redes internas corporativas, são percebidas ações provindas desse ataque que alteram o funcionamento normal do sistema e logo se vêm a tona as complicações causadas por este ataque a rede. As formas de ataque podem ocorrer das mais diversas formas – ataques provenientes do ambiente interno da instituição, ataque de vírus externos ou que por alguma forma os funcionários "importaram" tais vírus ao ambiente interno através de *pen-drives,* disquetes, DVDs, CDs... -, com as mais complexas formas de infecção – através de *worms,* Cavalos de Troia, *Phishing* - e diferentes meios de atuação deste *malware* – apenas descoberta de senhas e falhas do Sistema Operacional ou de outros programas, apenas publicidade do vírus ou até roubo de senhas e dados cadastrais. Porém, é preciso salientar que hoje prevalece o número de ataques com fins financeiros diferentemente dos motivos anteriores que eram dar visto ao conhecimento tecnológico do invasor e sua capacidade de "manipular" os mais complexos sistemas, "mandar" neles.

O ataque em si e os prejuízos causados podem ser mensuráveis de forma básica segundo valores exorbitantes de receitas deixadas de serem conferidas numa demonstração de resultado empresarial. Num outro prejuízo considerável, veremos um exemplo de parada de serviços numa entidade, deixando a ocorrência mais grave pelo fato desse interrompimento de serviços ser num ente de prestação pública. Conforme exemplo posterior, além de falhas em prestações de serviços, analisados posteriormente, outras formas de perdas podem ser percebidas e causar danos ainda maiores que os anteriormente falados: perdas de informações consideradas sigilosas por Estados Internacionais (Brasil, Estados Unidos, Alemanha...) cujas estruturações dependem de tais informações tanto num âmbito de defesa estratégica como armazenamento de estratégicos dados locais.

É importante inicialmente destacar a ocorrência cada vez mais corriqueira de ataques a sistemas computacionais, porém também deve haver uma análise sobre quais motivos ocasionaram tais fatores. Em alguns casos, de fato, é necessitado um estudo mais detalhado além de profissionais especialistas nos específicos casos, incluindo manipulação de programas específicos ou técnicas aplicadas segundo certificações peculiares. Haverá um foco maior nas falhas humanas e estas serão citadas principalmente - considerada por especialistas a parte mais frágil dentre os componentes necessários a garantir um sistema de informação com relevantes índices de segurança.

2.1 – Aumento de Produção de Pragas Eletrônicas e Ataques Realizados

Em 1984, Fred Cohen relata no seu paper “Experiments with computer viruses” a existência de programas maliciosos, nocivos ao sistema como um todo e batiza-os de “vírus de computador”. Apenas dois anos após, foi criado o primeiro vírus de computador batizado como Lahore, ou Brain-a, ou Pakistani dentre outros nomes conhecidos. Ele era um vírus de boot infectando assim o sistema de inicialização do disco rígido. Em 1988 são datadas as primeiras ocorrências de possíveis antivírus exatamente para defesa contra o Brain-a – este antivírus realizava tanto defesa como imunizava o sistema para futuros ataques.

Somados mais quatro anos, 80 vírus já eram conhecidos. O fato porém é que 10 anos após já eram relatados cerca de 49.000 vírus e em 2007 já eram percebidos mais de 150.000 vírus conhecidos. [3] Em março de 2009, 630.000 vírus. O fato é que o número de vírus está sempre crescendo numa proporção cada vez mais assustadora quando analisadas as variáveis formas de ataque surgidas, e as que estão a surgir, e os diferentes meios de ataques que nem sempre nossos sistemas de defesa estariam habilitados a efetivar a defesa pela nova forma de atuação ou de ataque de vírus.

Problemas em abril de 2009 causados num serviço de Internet chamado Speedy, fornecido pela Operadora Telefônica, causaram parada de funcionamento do respectivo serviço através de congestionamento dos servidores da operadora no Estado de São Paulo – mais precisamente numa cidade chamada Bauru. Posteriormente, segundo Eduardo Godinho, gerente técnico da Trend Micro, empresa que desenvolve softwares de segurança para computadores, houve constatação que o problema foi causado por ataque de um cracker. Denny Roger, diretor da Epsec, empresa que presta consultoria de segurança “desconfia que os ataques foram causados por um vírus ainda não identificado”. Segundo outro especialista, Gabriel Menegatti, diretor de tecnologia da F-Secure, isentando a Telefônica de qualquer culpa, comenta: “não adianta, você pode ter a tecnologia de ponta, e os crackers desenvolverem algo mais evoluído. É uma briga de gato e rato.” [4]

“Cerca de 60% de todas ameaças (de softwares malignos) dos últimos 20 anos surgiram nos últimos 12 meses”, disse Vicent Weafer, vice-presidente de informações e segurança de conteúdo da *Sysmantec*, em entrevista a agência *Reuters.* As formas de ataque também estão variando. As fórmulas utilizadas de ataques através de *spans* por e-mail, conhecidos como *phishing,* estãos sendo substituídas e os crackers exploram mais a invasão de sites de empresas sem setor técnico específico pela segurança, por exemplo, de uma empresa local e de menor porte. [5]

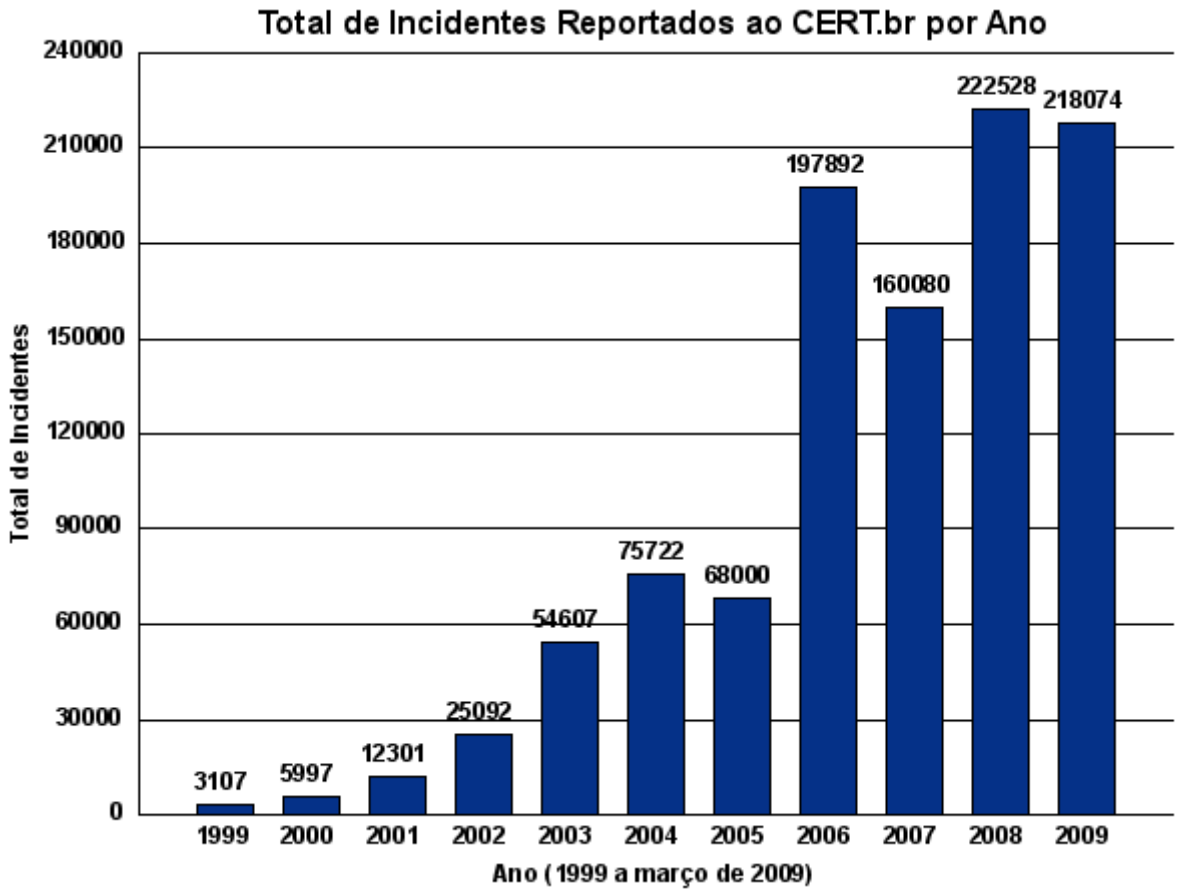


Ilustração 1: Total de Incidentes Reportados ao CERT.br por Ano

Segundo os dados do CERT.br - grupo de resposta a incidentes de segurança para a Internet brasileira responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil -, sobre o total de incidentes reportados a este, percebe-se uma tendência ao aumento do número de ataques – apesar de algumas diminuições no número de incidentes em períodos específicos – porém sempre se percebe o aumento posterior as diminuições. E, mais ainda, foi quadruplicado o número de ataques contando os últimos 5 anos – observando que em 2009 foi contabilizado apenas o primeiro trimestre.

Faz-se necessária destacar a importância dada aos ataques e a tendência, além do excesso de ocorrências que já existem, a massificação desta prática. Além de processos de roubos de informações, desafio sobre a quebra de seguranças de sistemas ou ganhar publicidade encima de uma praga sua, os ataques virtuais tendem a criar a chamada “Guerra Cibernética”, massificando a ocorrência de ataques virtuais. Segundo Parks e Duggan, sobre a Guerra Cibernética, “é o subconjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo

cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes.", "o mais relevante (destes mundos cibernéticos) é a Internet e as redes relacionadas, as quais compartilham mídias com a Internet....".[5] Países já buscam a especialidade nesta prática tendo em vista que os ataques físicos através de armamentos, veículos especiais de guerra e soldados, já são seguidos de ataques cibernéticos – ressaltando que o termo em si é associado a um patrocínio de possíveis Estados capazes de guerras físicas. Em 2007, ataques em série deixaram a Estônia sem serviços de redes – computadores de Partidos Políticos, de bancos e do governo foram os principais atingidos. A Geórgia, igualmente ao ocorrido na Estônia, em 2008, também teve seus serviços offline por momentos, porém tal situação foi seguida de invasão física do exército russo. [6]

2.2 – Diferentes tipos de ataques

Uma vez comentado o número crescente de vírus desenvolvidos bem como a ocorrência cada vez mais constante de ataques, são percebidas diversas formas de se produzir um ataque e diversos tipos de pragas virtuais que poderiam proceder com ameaça num sistema. Devemos conhecer as diversas formas de ataques e características que essas ameaças teriam por si sós.

Ressaltaremos a existência não apenas dos ataques realizados por softwares específicos nessa ação, porém outros provenientes, por exemplo, de um corte de eletricidade provocado buscando paradas de serviços e fragilidades no ambiente que, direta ou indiretamente, guardaria as informações. Uma ocorrência deste ataque ocorreu nos Estados Unidos quando hackers "entraram" na rede elétrica norte-americana deixando alguns softwares que seriam utilizados para prejudicar o sistema e monitorar a rede de energia. [38]

Será realizado uma maior explanação sobre os diversos tipos de ataque e diferentes manifestações. Nos ataques em que necessitem ser mais detalhados, os detalhamentos ocorrerão nas respectivas seções. Citaremos algumas delas:

- Vírus – Programa de computador que se hospeda num outro programa e visa infecção de arquivos. Sua ação dependerá então da execução deste programa hospedeiro - que não necessariamente terá extensão ".exe". Alguns também são programados para executarem num determinado momento. O vírus é capaz de se replicar num sistema podendo ele se espalhar rapidamente em diversas máquinas – tanto estando elas locais como localizadas na rede, incluindo Internet. Alguns vírus são capazes de excluir

arquivos, formatar discos rígidos e parar serviços. Vírus em si é este termo genérico não possuindo maiores pretensões de roubos financeiros ou de informações, apenas realizam corrupção de arquivos e programas. [7] Uma das formas de infecção por vírus ocorrerá através de *pen drives* infectados.

- Worm ("Vermes") – Software capaz de criar cópia de si próprio. Eles permitem que sejam difundidos de forma maciça se infectando por máquinas de todo mundo. Executado independente do sistema – não necessita que um certo programa seja executado para ficar ativado – são capazes de saturarem os recursos do computador e da rede impedindo assim que eles sejam utilizados. Anteriormente a ideia de utilização do worm era prover conhecimento ao(s) seu(s) criador(es) e sua capacidade de ser prejudicial ao sistema, hoje, porém, são orientados para crimes financeiros. A ideia do worm em si é que ele seja espalhado por várias máquinas e logo o cyber-criminoso terá controle de ações que podem ser executadas paralelamente pelas máquinas infectadas (ordenar que elas baixem arquivos maliciosos, lancem ataques de negação de serviço, etc). [7] Sua infecção ocorre principalmente através de vulnerabilidades nos programas causadas pela falta de atualizações neles.

- Trojan Horse – Mais conhecido no Brasil como "Cavalo de Troia". Percebendo então este sugestivo nome, este malware se manifesta fragilizando a máquina e favorecendo a ocorrência de ataques externos. Ele libera portas de comunicações sabendo que futuramente seu criador a utilizará em ataques. A infecção por trojan ocorre através de dissimulação deste Cavalo de Troia num programa que seria útil para o usuário. Ou seja, o próprio usuário instalará um programa que seria legítimo, porém estará instalando um trojan – instalação direta no computador. Sua manifestação depende da execução do Cavalo de Troia na máquina, geralmente há um "apelo" para que o usuário execute o programa, normalmente através de engenharia social. Vem contido geralmente em anexos de e-mails ou disponível em alguns sites.

- Engenharia Social – Nesse caso, o ataque será pouco, ou nada, baseado em programas de computador. Sobre a engenharia social, a tentativa de ataque ocorrerá sobre o fator humano. Serão pessoas que buscarão extrair informações do sistema das mais diferentes formas – através de conversas pessoais com operadores do sistema ou pessoas com dados de acesso ao sistema corporativo, através de ligações telefônicas fingindo ser outras pessoas, será através de e-mail pedindo dados sensíveis ou até mesmo verificando lixeiras físicas da instituição.

- Acesso físico: o atacante acessa fisicamente às salas e às máquinas dela. Exemplos desse tipo de ataque são os de corte de eletricidade, "sumiço" de computadores, peças e dados, escuta do tráfego sobre a rede entre outros.
- Intercepção de comunicações: Neste caso haverá alguma caracterização como usurpação de identidade, roubo de sessão e desvios e alterações de mensagens.
- DoS ("Denial-of-service") – Tentativa de indisponibilizar serviços numa dada máquina servidora. Uma vez esta máquina sem serviços disponíveis, as outras máquinas que dela dependeriam para tal, já não poderão se utilizarem desses – daí o termo "Denial-of-service", em português, negação de serviço. Nesta forma de ataque, um computador "mestre" terá uma série de máquinas "escravas" sob seu controle. Uma vez este "mestre" ativando o ataque, os escravos irão todos, ao mesmo tempo, requisitar algum serviço específico do servidor. Servidores costumam ter limites de conexões a serem atendidas (slots), logo o servidor se dedicará exclusivamente a essas requisições das máquinas "escravas" e nenhum outro "slot" mais estará livre para outras solicitações. [8]
- Keylogger (em português, registrador de teclas) realiza o monitoramento de tudo que é digitado. Normalmente infecta a máquina através de execução de outras formas de ataque – através de Trojans ou Spywares. Pode ser realizado também através de captura da tela do usuário tendo como foco o movimento do *mouse* nela. Após a coleta das informações, o envio ocorre principalmente através de e-mail ou Messenger. [9]
- Phishing – Técnica de roubo de identidade on-line, geralmente visando tomada de dados financeiros. Esta ocorrência se dá principalmente com a utilização de spam, websites maliciosos, e-mails e mensagens instantâneas. Abaixo, exemplo real de phishing em que se faria um possível restabelecimento de CPF. O usuário é induzido a baixar o arquivo malicioso IRPF2009win32v1.0.zip, que conteria este programa. Logo repassará as informações necessárias para a realização do phishing.

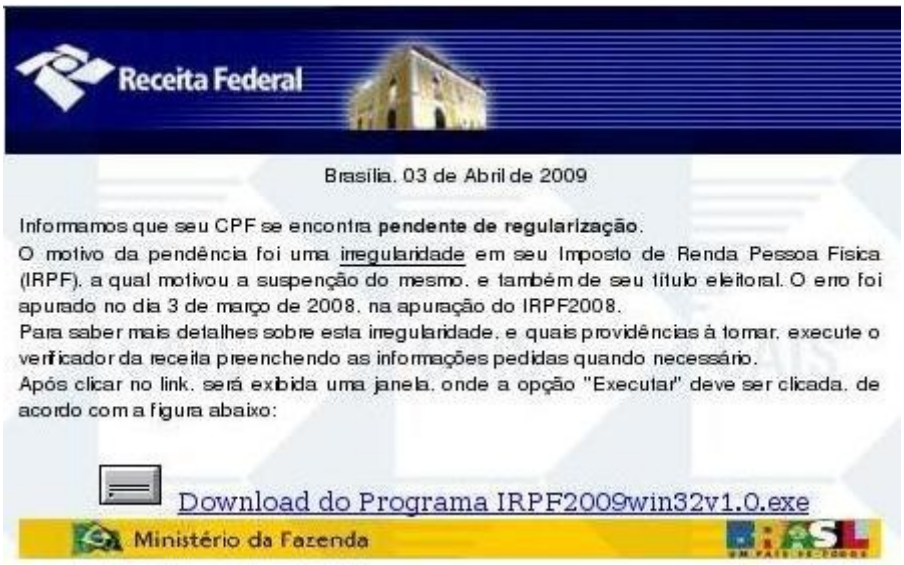


Ilustração 2: Phishing simulando correspondência da Receita Federal

Visando uma dúvida sobre a existência ou não de um ataque, estes tipos de ataques quando baseados no uso de software poderão vir acompanhados de disfarces para as possíveis ocorrências: Hoax – boato da existência de vírus; Mutante – mutação do arquivo contaminado a cada execução dele; Encriptados – encriptação do vírus dificultando a detecção deles.

Finalizando a análise sobre as diversas formas de ataques, destacaremos agora a 10ª Pesquisa Nacional de Segurança da Informação realizada em 2007 pela empresa Módulo. Neste quadro, foram postos os diversos problemas numa única tabela comparativa em que houve perdas financeiras ocasionadas. Os motivos então foram destacados: [2]

Ilustração 3: Problemas que geraram perdas financeiras

2.2 – Exemplos reais de ataques e perdas reconhecidas

O DETRAN-PE, Departamento Estadual de Transportes de Pernambuco, no início de Fevereiro de 2009, teve seus procedimentos parados por lentidão e falhas durante requisições de serviços internos. O resultado disto foi que seus serviços e atendimentos permaneceram parados por aproximadamente 3 dias – tempo suficiente para a imprensa estampar as "Matérias de capa" dos jornais e mais de 1.400 computadores terem seus sistemas operacionais afetados.[10] Sabe-se que o worm que causou tamanho prejuízo foi o Conficker. A forma de infecção em si e o suposto responsável por ela não foram constatados, porém acredita-se que, segundo o meio mais comum de infecção do vírus específico acontecer, algum pen drive infectado tenha sido posto numa máquina interna ao DETRAN-PE. Esta de fato é a versão mais aceita para esta infecção. O que chama a atenção é que, para o tratamento deste malware, bastavam os antivírus num correto funcionamento e os computadores da instituição com uma atualização disponível gratuitamente para sistemas

operacionais Windows.

Em 31 de Janeiro de 2008, um dos servidores Unix da Fannie Mae parou de responder as requisições a ele realizadas. Milhões de dólares foram perdidos juntos aos dados tendo em vista que o problema detectado em um único servidor, que já seria uma perda considerável, em pouco tempo já se espalhara por todos 4.000 servidores que nesta instituição se encontravam. Os trabalhos dela então foram parados durante uma semana. Este tempo de uma semana apenas não foi prolongado pela ação de um funcionário da Fannie Mae que acidentalmente percebeu o script malicioso em execução no sistema. Tamanho prejuízo foi causado pela ação intencional de um funcionário recém-demitido da empresa que escrevera um script e o deixou após sua saída da empresa [11].

Em 2009, nos primeiros 60 dias do ano e da Administração de Barack Obama, atual presidente dos Estados Unidos da América, um e-mail obtido pelo Projeto de Monitoramento Governamental revela um embaraçador fato ocorrido. Estão desaparecidos três computadores do Laboratório de Armas Nucleares Americanos localizado no Novo México/EUA. Esse fato está compreendido apenas nas três primeiras semanas do ano; há ainda mais de 70 outras máquinas sumidas anteriormente a esse período. Muito mais que a gestão de patrimônio material, o caso das máquinas roubadas sugere que há informações cujas suas existências se resumiam a estes computadores perdidos além de outro agravante: a hipótese de que sites *Off-line* ainda não estariam devidamente armazenados no Banco de Dados local tendo sido perdidos juntos as máquinas. Obama solicitou revisão quanto a administração local da cyber-segurança para uma tentativa de modificação completa e solução de tamanhos problemas. [12] Alguns questionamentos podem ser feitos. Qual política regulava a entrada ou saída de propriedade material da localidade? Segundo boas práticas da norma ISO 27002, seria preciso um inventário de ativos de informação a ser mantido. Um desses ativos seriam os equipamentos computacionais que visariam manter um outro ativo da instituição: a reputação e imagem dela. Outra questão a ser destacada: onde estariam os backups destas informações? Falhas essas graves e basilares causadas, dentre outros setores, pelo responsável pela segurança da informação local e seus métodos de trabalho.

No mês de Janeiro de 2003, um worm chamado Sapphire-Slammer causou uma verdadeira queda na disponibilidade de banda larga da rede mundial de computadores. O worm, em aproximadamente 8,5 segundos, foi capaz de duplicar o número de máquinas infectadas. Num tempo aproximado de 10 minutos já eram atingidas aproximadamente 90% das máquinas vulneráveis conectadas a *Internet.* Inclusive, entre as máquinas atingidas, estariam pelo menos 5 dos 13 servidores DNS por onde até então passavam todos os tráfegos da rede mundial de computadores. Este worm realizava ataques de negação de serviços – os chamados DoS. Dentre

tantas consequências e prejuízos causados pelo ataque, as reconhecidamente mais graves foram cancelamentos de voos em linhas aéreas, alteração na realização e falta de confiança em resultados de eleições ao redor do mundo, falhas em caixas eletrônicos que funcionavam em bancos, conflito de funcionalidades – ou seja, desligamento provisório - por 5 horas do sistema de segurança de uma usina nuclear no centro-oeste dos Estados Unidos localizada em Ohio. A vulnerabilidade que permitia este acesso do *malware,* eram falhas em dois produtos desenvolvidos pela *Microsoft*. O detalhe entretanto era que as vulnerabilidades já estavam devidamente mapeadas, tratadas e as correções já estavam disponibilizadas desde julho do ano anterior a ocorrência.[13] Pior: a própria *Microsoft* teve computadores infectados. Falha percebida: administradores de sistemas, ou responsáveis por atualizações, não haviam instalado o patch de segurança que teria evitado tamanha propagação.

2.3 – Fragilidade humana referente às falhas

Em comum entre os exemplos, podemos perceber falhas que vão além dos sofwares utilizados para segurança ou processos bem implementados e testados por estes. Percebe-se que a falha, independente da existência de software frágeis ou talvez a ausência destes, é marcada por alguma deficiência pessoal dentro de cada uma das corporações. Afinal, foram percebidas falhas basicamente dos funcionários e usuários, falta de treinamento correto dentro do capital humano que de alguma forma seria responsável pela segurança da informação. A ideia então que apenas tecnologia ou processos seriam suficientes para garantir um sistema de informação seguro é derrubada facilmente quando observados os exemplos do tópico anterior.

Reforçando a ideia dos exemplos citados, Bruce Schneier destaca a existência de três partes principais no processo de segurança: tecnologia, processos e pessoas. Ele ainda explica com considerável destaque a formação, à partir desses três elos, de uma corrente. Nessa corrente formada, uma parte corresponderia a um elo mais fraco: a parte humana. Não apenas Schneier aponta as pessoas como o elo mais fraco, porém esta é uma unanimidade entre diversos especialistas. [14]

Ratificando, 50% das invasões não se valem apenas da tecnologia, mas principalmente da fragilidade humana. Segundo Kevin Mitnick, considerado o maior cracker que já existiu, “A falta de segurança é um problema sério e, infelizmente, muitas universidades, empresas e muitos órgãos do

governo não se exercitam, não se atualizam. Eles deixam seus sistemas vulneráveis a ataques e não têm o mínimo de perspicácia para perceber falhas humanas, cada vez mais exploradas por hackers."[15] e mais uma vez há o destaque às falhas humanas e a mais explorada forma de ataque.

"Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis." [16] – completa Mitnick referindo-se a fragilidade humana independente de excesso de cuidados e investimento tecnológico na segurança da informação. Logo percebe-se a predominância, quando comentada por especialistas, da fragilidade humana como principal meio a ser explorado visando um ataque sobre as informações.

3 – Falhas humanas percebidas

É reconhecida a possível fragilidade causada pelo recurso humano segundo uma falta de treinamento ou até mesmo por possíveis más-intenções. Uma vez percebida essa fragilidade são destacados alguns tipos de falhas humanas as quais caracterizarão diversas formas dessa ocorrência. Importante destacar que serão utilizados os exemplos anteriores para associar aos diversos meios de falhas acrescidos por outros com menores detalhes porém que enriquecerão os dados e atestarão a ideia. Outro ponto de destaque é que muitas dessas ocorrências estarão correlacionadas. Assim será normal visualizar uma falha que seja perfeitamente percebida num outro tipo de falha. Falta de investimento humano-tecnológico poderia se confundir com a falta de treinamento ao recurso humano.

3.1 - Falta de treinamento ao recurso humano

Percebida a importância do recurso pessoal no cuidado a informação corporativa, faz-se necessário investimento na preparação humana sobre a segurança da informação. Essa educação deve ser realizada tanto em aspectos mais simples, como formas básicas de garantia de segurança da informação – observar se o antivírus está atualizado, evitar clicar em links duvidosos ou até não compartilhar senhas – como outras que exigirão um pouco mais de treino – um exemplo seria identificar possíveis comportamentos característicos de infecções de vírus num computador, numa rede, ou entender mensagem provenientes do antivírus da empresa e como agir na existência delas. Vale ressaltar também que a própria empresa pode ser responsabilizada quando não oferece o suficiente investimento na educação dos funcionários.

Ratificando a importância de treinamentos em segurança da informação, segundo o gerente de engenharia de sistemas da Symantec, é possível dizer que: “alguém querendo se dar bem com um dado sigiloso corresponde a apenas 5% dos problemas... o restante é falta de treinamento”. Percebida então a importância do treinamento da equipe como um todo, um outro dado preocupa quando avaliado destaque das empresas e importância que elas investem num treinamento de funcionários. Gerente regional da Kaspersky Labs no Brasil, Eljo Aragão, à partir de um relatório do FBI, aponta que “40% das empresas entrevistadas investem menos de 1% do budget voltado à

segurança da informação na educação dos usuários". Por isso, "é preciso de fato definir o que pode ou não, incluindo regras para uso de e-mail, e mostrar por que há um monitoramento ou bloqueio", aponta Aragão. [17]

Treinamentos incluiriam as mais diversas áreas e complexidades. Naturalmente que uma pessoa da informática teria um treinamento diferenciado em relação a uma pessoa cujo uso da informática seja menos frequente ou que não seja de fato o instrumento principal de trabalho da pessoa. Vale ressaltar que há funcionários que apenas acessam máquinas com finalidades pontais, para um uso específico de um determinado programa ou de um acesso a certo site. Como constantemente comentado neste trabalho, deve haver um trabalho conjunto visando todas pessoas que compõem a instituição.

No exemplo citado do DETRAN-PE, os funcionários não tinham noção da real situação do antivírus da empresa – estaria ele atualizado para tratar possível ataque do Conficker? Mais ainda, tendo em vista que o ataque ocorreu, os sistemas operacionais estavam desatualizados. Vale perceber que nem todos tinham a consciência destas desatualizações e, se tivessem, não tinham consciência da importância de se manter atualizado o Sistema Operacional e o antivírus bem como da importância de se manter o serviço público em funcionamento.

3.2 - Falta de investimento humano/tecnológico

A falha percebida referente a ausência, ou baixo, investimento tecnológico se enquadra mais em falhas encontradas sobre os possíveis diretores, chefes, gerentes, ou seja, pessoas responsáveis pela administração de outras pessoas e dos produtos da tecnologia.

Uma questão principal pode ser destacada: qual o indicador quanto ao lucro conseguido com o procedimento utilizado de segurança? Uma empresa costuma aferir a utilidade de alguns produtos, e assim a aquisição do produto, segundo um simples critério – este software aumentou minha lucratividade através de diminuição de despesas ou aumento de receitas? O maior problema nesta comparação é o fato de ser complicada a estimativa referente a esses números. É difícil a estimativa sobre a real economia causada pela utilização de um novo antivírus, ou IDS, ou Firewall, ou treinamento pessoal. O sistema está seguro pelo fato do investimento ter evitado ataques – valeu o investimento - ou não ocorreram tentativas de prejudicar o sistema – não teve lógica o investimento?

Tendo em vista isto, investimento em segurança da informação não poderia ser tratado como um tipo qualquer de investimento. A segurança da informação não é associável a bens tangíveis ou então retornos mensuráveis segundo as formas tradicionais de indicadores. Um fato porém é destacado. Segundo estudos, a maioria das empresas enxergam o treinamento voltado especificamente para a área de segurança da informação como algo importante, porém os respondentes, setores em geral, afirmam não acreditarem ser suficiente o investimento que é realizado na área. [18]

Investimento deve ser realizado não apenas para evitar possíveis ocorrências de segurança. Deve-se perceber a priori que um investimento também terá a função de garantir que um outro dispêndio de capital consiga valer realmente os gastos realizados. Um exemplo, baseado num panorama mais crítico, é quando observa-se alguma das soluções de segurança da informação mais utilizadas. Alguns meios de segurança como sistemas criptográficos, assinaturas digitais, uso de VPN's, análises de vulnerabilidades, uma vez apresentando ausência de investimento nessas áreas, comprometeria parte ou todo investimento e o esforço dispendido na instalação e implementação da segurança. [19]

Observando a questão do Laboratório de Armas Nucleares Americanos no Novo México, EUA, não foram realizados maiores investimentos quanto a segurança física dos ativos de hardware. A ausência de possíveis câmeras de segurança ou sensores de presença ou controle de acesso às salas não obtiveram quaisquer vestígios do incidente. O desaparecimento frequente dos computadores põe a prova o sistema de segurança do órgão bem como falhas que seriam supridas pelo correto investimento sobre produtos ou treinamento de pessoas.

3.3 - Falhas humanas

Quando se abre uma possível porta que facilite entradas de malwares em ambientes gerais ou diretamente a dados internos da empresa, muitas precauções poderiam ser tomadas por simples treinamentos referentes a boas práticas de utilização da rede interna. Alguns erros são básicos e com considerável ocorrência e prejudicidade. Serão, inicialmente, destacadas algumas das falhas mais comuns cometidas pelas pessoas de uma empresa no âmbito de usuário num sistema de informação. Posteriormente falhas cometidas na implementação do segurança pelos administradores dela.

Citaremos falhas cometidas pelos usuários e funcionários:

- Clicar em links maliciosos – Quando a empresa não impõe limites quanto a navegação, é comum a prática de clicar em links sem maiores critérios. Funcionários imaginam que clicar em tais links no ambiente empresarial, independentes sobre serem ou não maliciosos, não irão ocasionar maiores problemas. Imaginam o ambiente de defesa da empresa "infalível" pela existência de antivírus e *firewall;*
- Cuidar mal de senhas – Se cada funcionário tem senha própria, supõe-se que esta seja a identificação dele para algum procedimento, algo que o ligará a certas ações. Isto as vezes passa despercebido por funcionários que compartilham senhas, consequentemente, informações exclusivas de cada. E, à partir dessa falta de cuidado com senhas percebido pelo compartilhamento delas, muitas vezes acabam "autorizando" utilização de serviços que apenas a identificação dele seria possível;
- Senhas fracas ou únicas. Senha fraca significa que esta é facilmente descoberta – há programas, inclusive, específicos para tais práticas. Uma senha forte dificilmente será quebrada inclusive por programas específicos para tal. Senhas únicas referem-se a repetição de senha em diversos serviços diferentes – e-mail empresarial, acesso ao sistema, acesso a outros programas, etc; [21]
- Encaminhar arquivos profissionais para e-mails pessoais – mesmo que não seja por má-intenção - é uma falha ocorrida comumente. Muitos usuários querem enviar dados para e-mail pessoal visando sua utilização no ambiente residencial para assim adiantar serviços profissionais. Porém o e-mail que antes era enviado através de meios seguros numa rede interna, VPN (*Virtual Private Networks)* ou intranet. Estes ainda estariam associados com procedimentos de segurança, como assinaturas digitais ou criptografias, serão transmitidos pela Internet sem procedimentos de segurança necessários saindo de um meio seguro para outro vulnerável;
- Navegações muito pessoais – Mais uma vez o usuário imagina que o ambiente empresarial estará livre de quaisquer infecções. À partir de então, há acesso de redes sociais, lojas virtuais e utilização de *bankline* em excesso. Dados pessoais podem ser acessados e roubados prejudicando tanto empresa como o próprio usuário. [20]

Estas foram apenas algumas das falhas mais comuns percebidas dos usuários do sistema. Porém num âmbito mais voltado aos administradores da segurança, ou que deveriam ser

responsáveis por tal, também cometem falhas que poderiam ser evitadas por procedimentos básicos. Pode-se destacar que a maioria dos problemas que vulnerabilizam uma rede está relacionada a um conjunto básico de falhas tanto na implantação quanto no desenvolvimento do processo. Algumas falhas serão destacadas:

- Ausência de procedimentos de segurança. Neste ponto se destaca a ausência de uma política de segurança, procedimentos e normas. Na ausência de legislação brasileira sobre existência de leis sobre utilização digital da informação, é necessário que a própria empresa limite a este uso pelos funcionários;
- Planos de continuidade improdutivos – ou a ausência deles. Um plano de continuidade deve ser dinâmico e sempre atualizado. Deve mais que isso ser testado e abranger cada vez mais o escopo e os cenários da empresa;
- Cópias de segurança. O ambiente da tecnologia precisa ser recuperado em determinadas situações. Não apenas para concertar falhas ocorridas nos tratamentos da informação, porém incluir a recuperação em situações de perda dela, causados de forma intencional ou acidental;
- Não existência de gestor de segurança da informação. Naturalmente que este deve ser especializado no assunto. Ele que se dedicará ao gerenciamento da segurança computacional;
- Não alinhamento do negócio com a segurança. É um grande desafio conscientizar a instituição que todos negócios devem estar alinhados com o setor específico pela segurança da informação. Mais que isso, esta deve ser entendida de forma prioritária quando na definição de novos processo de informática;
- Pouco treinamento e conscientização. Cada usuário precisaria ser treinado e conscientizado de sua importância e suas responsabilidades. Logo a falha do usuário pode ser associada ao próprio administrador da segurança. [22]

3.4 - Fragilidade frente engenharia social

A Engenharia Social é uma prática que visa a obtenção de informações importantes ou que

tenham um conteúdo mais sigiloso por pessoas não autorizadas a obter tais informações. Esta obtenção ocorre por meio de enganação e pela exploração da confiança das pessoas. Esta forma de ataque apresenta um foco na exploração ao recurso humano sem tantas preocupações com utilização de força bruta e exploração de erros das máquinas.

Buscando uma definição para a engenharia social, segundo a cartilha de segurança da CERT.Br, poderíamos destacar que é "um método de ataque onde alguém faz persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter tais informações que podem ser utilizadas para ter acesso, não autorizado, a computadores ou informações".

Nesse tipo de ataque, o engenheiro social (a pessoa que pretende roubar a informação) trabalhará focado em aspectos psicológicos humanos. Sentimentos como insegurança, medo, ingenuidade ou o simples aproveitamento de um desejo do usuário serão explorados por ele visando o roubo da informação. Segundo o diretor especialista de pesquisas do *Gartner Research,* Rich Mogull, "essa é a maior ameaça à continuidade dos negócios para a próxima década" (*InformationWeek* Brasil, 2003). De acordo com o analista Edgar D'Andrea, sócio da *PricewaterhouseCoopers* na área de soluções de gerenciamento de risco "'a engenharia social oferece resultados até mesmo sem grande esforço, porque as pessoas tratam o tema com ingenuidade'" (*InformationWeek* Brasil, 2003).

As formas de ataques serão das mais variadas: tanto contato corpo-a-corpo, como conversas telefônicas e e-mails podem ser utilizados na aplicação do roubo da informação. Outro ponto importante é que o a pessoa atacada costuma não ter a exata noção da importância da informação será atacada. Logo o fornecimento de uma senha estratégica seria um simples acesso de uma série de dados sem maiores interesses. Será explorado, finalmente, a pouca compreensão do usuário quanto a grande importância da informação que ele poderá fornecer a um estranho.

"É incrível como é fácil para um engenheiro social convencer as pessoas a fazerem as coisas com base no modo como ele estrutura a solicitação. A tese é acionar uma resposta automática com base nos princípios psicológicos e utilizar os atalhos mentais que as pessoas usam quando percebem que o interlocutor é um aliado" [23]

Mais ainda, reforçando a ideia de fragilidade humana frente esta engenharia, escrito no livro A Arte de Enganar: "As empresas que realizam testes de penetração de segurança relatam que suas tentativas de invadir os sistemas de computadores de uma empresa cliente com métodos da engenharia social têm um índice de sucesso de quase 100 por cento". [24]

Tendo em vista então todas essas ideias especializadas quanto a fragilidade causada pela

engenharia social num sistema, faz-se necessárias as palavras que bem resumem a ideia do criminoso: “Sistemas de segurança feitos para proteger computadores e redes de investidas criminosas são desenhados por PhDs, codificados por especialistas de segurança com grau de mestrado e integrados nos ambientes corporativos de computação por técnicos habilitados treinados especificamente para aquele propósito. Neste especializado processo de segurança os usuários são freqüentemente esquecidos no fim. O fato simples e triste é que a probabilidade de se quebrar um código feito por um professor de matemática é muito mais baixa do que a probabilidade de se conseguir a senha da secretária de um chefe numa conversa. Se você fosse um atacante, onde você colocaria sua energia?”, e ainda completa, “Amadores atacam sistemas, profissionais atacam pessoas (...) Em realidade, ninguém pode depender da tecnologia para se fechar a porta aos ataques. Nenhuma solução de software pode resolver todos os problemas de segurança de computador que nos assombram, não importa o que o vendedor de software diga. Nós podemos depender somente de nós mesmos. No fim do dia, um computador é tão seguro quanto a pessoa que o utiliza esteja consciente e pronta para enfrentar os perigos que ela terá de encarar” [25]

3.5 - Más-intenções

Várias características de falhas humanas foram destacadas até agora. Porém todas tinham como base a falta de preparo dos funcionários da própria instituição, seja por ignorância ou falta de treinamento específico da empresa para as situações específicas dela. Uma outra forma de fragilização ganhará destaque. Um ataque cuja causa deste seja provocada pelas pessoas da organização destacando a má-intenção dos próprios funcionários da empresa que por algum motivo, principalmente os demitidos ou no limite de sua demissão, conforme os casos a serem citados ou recuperados deste trabalho, costumam agir de forma a prejudicar ou se aproveitar de informações ou conhecimentos de sistemas que garantiriam acessos privilegiados a serviços essenciais, críticos do sistema.

Seria possível um ex-funcionário entrar numa empresa de grande porte, cumprimentar a guarda obtendo livre acesso – afinal, tem aparência conhecida no ambiente interno – e ainda conseguir extrair informações estratégicas de outros funcionários se passando por um possível consultor em fase de auditoria? Um pouco complexo imaginar que essa série de ocorrências combinadas com falhas poderiam ocorrer, porém tal exemplo foi citado pela ISO – Internation

Organization for Standardization – e por Abby Christopher na Network World em maio de 2003. [20]

Segundo pesquisa, o índice de roubos de informações por funcionários demitidos ou que simplesmente deixaram seus empregos chega a 69% nos últimos 12 meses. Entre outros números a destacar, aproximadamente 61% dos funcionários demitidos que tinham uma visão negativa da empresa realizavam tais roubos. Entre as ações consideradas mais corriqueiras que caracterizavam roubos de dados, podem ser citadas levar informações de e-mails e copiar arquivos empresariais. Essas pessoas que roubavam as informações tinham três principais ideias quando interrogadas sobre o motivo do roubo:

- "Todo mundo faz isso"
- "A informação pode ser útil no futuro"
- "A companhia não pode rastrear o conteúdo até mim"[26]

3.6 - Ignorância dos usuários

De início haverá caracterização sobre o que seria um erro humano e uma ignorância de um usuário bem como compará-los e posteriormente saber qual a diferença deles. Adotando-se a Teoria da Confiabilidade de Almeida Junior, o conceito de erro humano se relaciona com os conceitos de falha e disfunção. O erro humano é uma conseqüência natural do processo de solução de problemas, assim como o é a própria ação correta.[27] Ou seja, é tentada uma ação visando o correto, buscando algo exato, porém, conforme a realidade, é normal o cometimento de erros.

Em contrapartida, poder-se-ia falar da ignorância humana. Esta seria caracterizada pelo fato de pessoas com discernimentos médios necessários serem capazes de identificar que tais atitudes não seriam cabíveis em determinadas situações, ou seja, caberia também verificar a capacidade de aplicação mínima de conhecimento em tais situações. É fácil imaginar que é algo comum não se fornecer senhas de serviços em geral na Internet. Porém quantas pessoas não costumam colar a senha no monitor ou simplesmente anotá-la num local de fácil acesso, as vezes ao lado da mesa do computador? Mais ainda, quantas pessoas não deixam perfeitamente anotado não apenas a senha de acesso a algo, porém todas informações pertinentes a usuários, a perguntas secretas e até passo-a-passo sobre como utilizar estas informações somadas a tais procedimentos na Internet. Talvez tais

ideias sejam totalmente aceitas quando o manipulador das informações seja uma pessoa com um nível menor de conhecimento no assunto e nos riscos destas formas de agir. Até mesmo esta pessoa, de certa forma, ter menor capacidade de raciocínio e conhecimentos provenientes de pouco estudo ou leitura (supondo uma recém e inexperiente secretária sem treinos e com pouco conhecimento de informática contratada numa empresa menor, informal), porém seria difícil imaginar um especialista em segurança da informação oferecer tais fragilidades. Isto caracterizará a ignorância de um usuário, ou seja, erros que não seriam desculpáveis pelo nível intelecto esperado da pessoa. Seriam situações que se imaginam ser muito simples de serem concluídos pela reação lógica básica as suas ocorrências.

Como se imaginar, por exemplo, que pessoas com consideráveis conhecimentos gerais e até especialistas na área de direito capazes de assumir os maiores postos no Poder Judiciário seriam capazes de se abismarem ao "conhecer" que senhas pessoais, independentes se senhas de bancos ou e-mails pessoais, na Internet não poderiam ser repassadas a ninguém além do titular. Mais ainda, se espantarem ao saber que a senha bancária não deveria ser repassada a ninguém além do titular. A resposta seria ainda mais espantosa: "eu costumo fornecer minha senha bancária inclusive aos funcionários terceirizados". E logo não apenas simples senhas pessoais estavam expostas, porém também senhas bancárias já seriam facilmente roubadas.

Numa outra ocorrência, uma segunda pessoa, também especialista na área de direito e também ocupando um dos maiores postos do serviço público, aproximadamente em novembro de 2007, ligaria para o setor responsável pela segurança da informação de um órgão público solicitando a liberação de determinado site com conteúdo adulto além de websites contendo músicas para serem copiadas de um servidor de procedência desconhecida localizado na Internet. Neste caso, houve um predomínio do desentendimento, ou simplesmente o fingimento de não conhecimento, sobre o risco de se disporem sites contendo tanto conteúdo adulto, geralmente associados a contaminações virtuais, como distribuição de músicas, outra forma de envio de contaminações. Segundo pesquisa realizada pela Revista Veja do dia 20 de maio de 2009 de uma escala de 1 à 10, foi avaliado em 9 os riscos causados pela visita a sites pornográficos e 7,5 o download de músicas ou vídeos em redes de compartilhamento de arquivos. [28]

Uma terceira ocorrência seria a elaboração de políticas de segurança da informação, esta será vista posteriormente, e a disponibilidade dela na rede mundial de computadores. Nesta política estariam demonstradas todas informações específicas de utilização da rede e de todos intervalos de IP's. Não apenas os Protocolos de Internet estão disponíveis, porém todas informações necessárias ao conhecimento específico da topologia da rede e todas estratégias administrativas sobre os ranges de IP. Esta política foi criada e está sobre administração de especialistas em informática e mesmo

assim permanece disponibilizada na Internet.

Finalmente, numa instituição também do Poder Judiciário, foi repassado um e-mail para todos funcionários da informática com solicitação de "atualização" de informações constantes num possível cadastro do Banco do Brasil. Este e-mail solicitava atualização de dados que tinham foco em dados bancários. Entretanto, existe instrução explícita no site do mesmo banco afirmando que nenhum e-mail é enviado aos seus clientes com solicitações de informações bancárias nem muito menos com atualizações além da natural exposição de tais informação nas diversas mídias informativas. O e-mail não tinha quaisquer "maquiagens" que o classificasse como ser realmente do site, apenas o texto em si. Esta mensagem foi repassada por um funcionário concursando exatamente da área de informática especializado em tal. Mesmo assim repassou o e-mail aconselhando a atualização de todos.

Todas as quatro situações foram presenciadas pelo autor deste trabalho e maiores detalhes das pessoas e do ambiente foram evitados como garantia a privacidade e imagem das pessoas e das respectivas instituições. Outro ponto destacado é não oferecer possíveis detalhes das deficiências nos órgãos.

Vale ressaltar que as ocorrências foram caracterizadas pelo fato um tanto quanto simples de serem concluídos ser certos ou errados proceder de tais formas. Basta agir com o mínimo bom senso segundo os mínimos conhecimentos, além da divulgação na imprensa, para saber a resposta sobre:

- Posso repassar minha senha de banco?
- Devo disponibilizar na Internet todas informações de minha rede local?
- Na minha instituição, baixar músicas e disponibilizar sites de conteúdo erótico seriam riscos de segurança?
- Devo atualizar imediatamente meus dados bancários quando houver solicitação destes por e-mail?

3.7 - Falha dos implementadores do software

A falha humana também pode ser percebida à partir de uma visão baseada nas pessoas que implementaram o sistema e dos usuários específicos, que utilizam de forma finalística este programa. Vale ressaltar que uma das diversas formas de ataque, como citado no tópico 2.2, "Diferentes tipos de ataques", é a exploração de vulnerabilidades deixadas, geralmente de forma

involuntária.

Porém, por que existem estas falhas de segurança? Algumas considerações podem ser feitas quando pensado nesta pergunta. Qual motivo dos programadores escreverem códigos inseguros? A solução seria a conscientização, seria o conhecimento dos gerentes e dos programadores sobre a importância no desenvolvimento de programas de forma segura, seria o estímulo a especialização em desenvolvimentos de aplicações com devidos procedimentos. Alguns fatores que contribuem para a insegurança serão citados:

- Livros de ensinamentos básicos de programação não costumam enfatizar procedimentos de segurança conforme outros procedimentos que costumam ser veemente enfatizados por eles. Exemplificando, um livro utilizado no ensinamento de programação na linguagem Java (Java, como programar. H. M. Deitel e P. J. Deitel; trad. Carlos Arthur Lang Lisbôa. - 4ª ed. - Porto Alegre: Bookman, 2003) apresenta várias dicas de programação paralelas ao ensinamento da linguagem. Essas dicas falam de:
    - Erros comuns cometidos na escrita do código;
    - Boas práticas de programação;
    - Dicas de testes e depuração;
    - Dicas de desempenho;
    - Dicas de portabilidade;
    - Observações de engenharia de software;
    - Aparências e comportamentos.

  Destes, nenhum citará, segundo apresentação do próprio livro além de leitura dentre estas dicas esparsas no material, tópicos de segurança.
- Poucas auditorias focadas na segurança. Exceto em programas que foquem especificamente na segurança de sistemas (antivírus, IDS, Firewall) ou estejam acompanhados por técnicos especializados dedicados ao tema, e mesmo assim não há uma garantia de qualidade suficiente referente a segurança, são raras auditorias e acompanhamentos que procurem possíveis falhas de software dos programas em desenvolvimento ou em produção.
- Poucos cursos especializando em segurança computacional;
- Programadores costumam ter outras preocupações consideradas prioritárias sobre a segurança. Qual a importância maior? Entregar um software no prazo ou entregar um

software com quantidade ínfima de falhas? O mercado exige cada vez mais a agilidade de entrega de produtos, mesmo que algumas vezes isto custe excesso de falhas no programa. Se falhas comuns de um software são deixadas de lado em nome da entrega do produto, o que se dizer então da segurança – tema um tanto quanto específico – que exigirá testes específicos;

- Usuários não costumam se preocupar com boas práticas de uso. A importância de fato, será a utilização do sistema. Outros procedimentos de bom uso de software - por exemplo, evitar deixar aberta uma seção com seu log – costumam ser esquecidas.
- "C" é uma linguagem considerada insegura. A insegurança por si só não seria o suficiente para contaminar um sistema, porém vale destacar a frequência de utilização da mesma linguagem.

Position May 2009	Position May 2008	Delta in Position	Programming Language	Ratings May 2009	Delta May 2008	Status
1	1	=	Java	19.537%	-1.35%	A
2	2	=	C	16.128%	+0.62%	A
3	3	=	C++	11.068%	+0.26%	A
4	4	=	PHP	9.921%	-0.28%	A
5	5	=	(Visual) Basic	8.631%	-1.16%	A
6	7	↑	Python	5.548%	+0.65%	A
7	8	↑	C#	4.266%	+0.21%	A
8	9	↑	JavaScript	3.548%	+0.62%	A
9	6	↓↓↓	Perl	3.525%	-2.02%	A
10	10	=	Ruby	2.692%	+0.05%	A
11	11	=	Delphi	2.327%	+0.30%	A

Ilustração 4: Linguagens de programação mais inseguras – TIOBE Software

Como se observa, a linguagem C é a segunda mais utilizada linguagem de programação segundo a TIOBE Software, atualizada neste mês de maio. Segundo o ranking, 16.128% das aplicações são projetadas na respectiva linguagem. [29]

- Segurança é "caro" (visando apenas o valor que precisa ser investido) e exige uma quantidade de tempo despendido. É difícil a previsão quanto ao lucro gerado pela implantação de um sistema seguro. Indicadores costumam medir o quanto tal medida foi

utilizada na economia de despesas ou aumento de receita – principal argumento de compra de um software por uma empresa. Logo é difícil estimar se o sistema não sofreu ataques por não ter sido de fato atacado, ou pela simples ausência de ocorrência de incidentes. Logo considera-se caro despender um certo tempo na implementação cuja preocupação será a segurança do sistema; mais ainda, implementação de softwares costumam exigir um tempo a mais de testes cuja dedicação seria focada na segurança do programa.

Ainda sobre a importância de um desenvolvimento de software e implementação segura e uma base para a solução desta questão, Wang e Wang apontam para a necessidade de qualidade de software agregada a segurança. Para estes dois, abordagens adequadas à segurança são feitas por meio de padrões e políticas, com o uso de bibliotecas e ferramentas de desenvolvimento e por meio da gestão administrativa do ciclo de desenvolvimento de sistemas e ferramentas físicas de manutenção. [30]

Tryfonas, Kiountouzis e Poulymenakou salientam, do mesmo modo, que a segurança da informação deve ser inserida nas etapas de desenvolvimento de software. Os autores apontam a necessidade de um mercado global de segurança da informação e advogam que os níveis de práticas de segurança devem ser os mesmos níveis do planejamento organizacional (estratégico, tático e operacional), lembrando ainda sobre a dificuldade de uso de políticas para a efetiva segurança da informação. [31]

4 - Procedimentos de defesa

Uma vez vistas as formas de ataque e os diversos tipos de falhas humanas, serão propostos alguns procedimentos que seriam necessários e até alguns suficientes para suprir as falhas cometidas cujos exemplos foram comentados neste trabalho.

Antes porém, faz-se necessário saber que, como citado anteriormente, novas pragas virtuais tendem a ser criadas sempre. Com isso, a defesa do sistema deve ser atualizada constantemente – tanto no sentido tecnológico como no conhecimento e atitudes humanas sobre os riscos. Seria possível ter um computador infalível contra ataques? Existe algum software, ou conjunto de softwares, que utilizados juntos aos maiores especialistas de informática garantiriam um sistema 100% seguro? A resposta é simples: não. Urnas eletrônicas no Brasil, exemplo de sistema que precisa dos maiores níveis de segurança, é ligada simplesmente na eletricidade, nenhuma ligação a mais. Esta poderia ser a forma ideal de segurança. Mais radicalmente ainda, viria a máxima: "Um sistema desligado é um sistema seguro".

Entretanto, de início, não se pode falar da segurança da informação sem citar os três itens básicas para o provimento de um ambiente seguro. Estes três itens, muitas vezes chamados de CIA (referência as primeiras letras dos itens no idioma inglês que são Confidencialidade – *Confidentiality -,* integridade – *Integrity* - e a disponibilidade - *Availability*) serão comentados: [32]

(a) Confidencialidade - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

(b) Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição).

(c) Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Os esforços e investimentos não podem estar exclusivamente associados a garantia da segurança da informação através da tecnologia. As ameaças de fato existem, sendo um tanto quanto dinâmicas as formas que elas atuam e se renovam. Uma infra-estrutura nos mais diversos aspectos é frágil e, por si só, um sistema perigoso.

Alguns procedimentos de defesa serão citados neste capítulo como:

- Organização da Segurança da Informação
- Política de Segurança da Informação funcionará como as regras, as leis, da utilização do sistema como um todo. Será obrigação aos usuários da rede agirem segundo o que na política estiver estabelecido deixando bem claro que nenhum usuário pode alegar falta de conhecimento destas normas tendo em vista estar ela explícita para qualquer pessoa e aprovada por toda instituição;
- Treinamento/educação ao recurso humano deve atingir a correta utilização da rede interna e formas de defesa. Deve-se buscar conscientização dos usuários e dos funcionários acerca da importância de um sistema seguro e da atuação de cada um. Atualização da ocorrência de vírus no cenário atual da Internet e destacar ocorrência de ataques associadas a novos procedimentos de defesa.
- Procedimentos básicos preventivos. Alguns procedimentos simples que pouco há preocupação nas instituições de defesa do sistema. Vale salientar que muitos procedimentos, apesar de básicos, são ignorados ou até entendidos como “algo que já está 'implícito' que sabemos”, ou como algo que “não precisamos focar em coisas simples assim”.
- Segurança Física, conforme visto nos exemplos acima, é essencial para o correto funcionamento da segurança lógica. É o início para um sistema seguro. Deve-se garantir segurança na empresa como um todo, mais ainda, o acesso aos sistemas lógicos e salas estratégicas da empresa devem ser controlados e monitorados;

4.1 - Organização da Segurança da Informação

Para o profissional da segurança da informação parece muito claro a importância que esta

representa para a empresa. Deve-se haver um cuidado quanto a organização pois muitos acabam incorporando em excesso estas características e logo criam uma visão contraditória, doentia, quando comparada a visão dos outros profissionais da instituição. Em certas ocasiões, não ocorre de fato esta caracterização de forma tão excessiva, porém mesmo as atitudes que aparentam mais cuidado dos profissionais da área, podem ocasionar descontentamento de outros setores. Como entender que meu programa trazido de casa, que me ajudaria num certo serviço da empresa, não estaria homologado pelo setor de segurança? Como poderia compreender que todos acessos físicos às salas das mais diferentes importâncias necessitariam verificação de permissão e autenticação? Por que aquele site, aparentemente inofensivo, está bloqueado? E este antivírus institucional que deixa minha máquina super-lenta? Vale ressaltar também, que os colaboradores não se sentem confortáveis em serem, de certa forma, controlados e policiados em seus trabalhos.

Por conta disso, os conflitos entre os funcionários de segurança e os diversos departamentos dentro das organizações são razoavelmente frequentes. Logo, o ambiente estaria favorecido para ocasionar insucesso nesta posição de cautela nos cuidados das informações. [33]

São muitos os desafios a serem encontrados pelos gestores da segurança, segundo a 10ª Pesquisa de Segurança da Informação realizada pela empresa Módulo[2], foram citados os principais obstáculo para a implementação da segurança da informação. Citaremos eles:

- Falta de conscientização dos executivos e usuários (pasmem, indicado por 55% dos entrevistados);
- Falta de orçamento (28% dos entrevistados);
- Falta de profissionais capacitados (8%);
- Falta de soluções específicas para minha necessidade (3%);
- Falta de ferramentas no mercado (2%).

Outros desafios são citados pelo livro Seccurity Officer [33]:

- Questões políticas;
- Administrar ambientes em que a ocorrência de incidentes urgentes é constante, comprometendo o planejamento de longo prazo.

Tendo em vista tamanhos desafios e complexidade quanto na proposta de um sistema de segurança, é proposta uma divisão a qual irá gerir e dividir os trabalhos em três níveis de atuação – visa principalmente empresas de médio e grande porte:

1. Estratégico – Planejamentos de longo prazo. Definição de objetivos e abordagens para o alcance daqueles planejamentos que servirão de guia para todos colaboradores. Aqui serão buscadas informações para o desenvolvimento da Política de Segurança da Informação – ou seja, aqui estará o apoio para valer medidas nem sempre populares, além dos recursos financeiros para elas.
2. Tático – Elaboração de iniciativas alinhadas com os objetivos anteriores – onde de fato é tomada a decisões reais. Trabalho mais focado no médio prazo, gerenciando a divisão de tarefas e atribuições dos respectivos colaboradores visando o sucesso da iniciativa. Onde serão desenvolvidos e implementados projetos de melhoria da segurança.
3. Operacional – Tarefas diariamente realizadas na organização. Todos departamentos realizarão elas segundo suas atribuições. Vale ressaltar que o setor responsável pela segurança deve atuar garantindo a mínima qualidade nos departamentos buscando sempre uma otimização nos resultados.

Para efetivação da referida divisão deve-se haver uma equipe de segurança da informação, muitas serão as características particulares dos participantes, cargos, de uma equipe de segurança, independente do seu tamanho ou forma de organização da empresa. É possível a reunião de mais de uma função num único profissional, porém deve-se haver a preocupação em possíveis conflitos em mais de uma função ocupadas por um mesmo profissional quando estas funções sejam incompatíveis ou quando uma realize auditoria na outra – por exemplo, o Gestor de Segurança ser a mesma pessoa que o Auditor de Sistemas de Informação.[33] Citaremos os membros da equipe:

- Chief Security Officer (Gestor de Segurança) - Mais alta posição hierárquica. Ocupa posição estratégica, chegando a tomar decisões condizentes com cargos executivos. Podendo inclusive chegar a solicitar remanejamento de recursos de outras áreas realizando negociações.
- Consultor de Segurança – Estará mais responsável pela execução de tarefas, diversificando conhecimento nas diversas áreas de segurança da informação. Foca-se mais em atividades estratégicas como na elaboração da Política de Segurança da Informação ou a execução de uma análise de risco.
- Analista de Segurança – Profundo conhecimento de alguma tecnologia específica

balanceado com sua visão de segurança.

- Auditor de Sistemas de Informação – Avaliação do funcionamento de um sistema de informação mesclado com o aspecto da segurança de informação.

Acompanhando o Gestor de Segurança da Informação, um Comitê de Segurança da Informação é proposto. Este grupo teria a função de tomar decisões estratégicas a respeito da segurança, elaborar diretrizes a serem seguida mostrando suporte e força para decisões e deliberar sobre aspectos que envolvam alta direção através de pareceres. Formado geralmente por diretores e executivos das mais diversas áreas, a ideia é representar a visão e preocupação dos diversas departamentos. Ocorrendo isto de forma verdadeira, algo um tanto quanto raro de ocorrer, o sucesso costuma ser considerável.

Sobre a posição numa estrutura organizacional numa situação ideal, a Segurança da Informação deveria reportar-se diretamente ao comando da empresa. Apenas para vias de comparação, em 2007, cerca de 25% das áreas de Segurança estavam ligadas a Administração ou Presidência enquanto 59% estavam ligadas às áreas de Tecnologia.[2] Tamanha relevância de subordinação apenas ao alto escalão é bem diferente do que se observa atualmente em que a consciência das empresas sobre os problemas de segurança é pequena relegando ela a um segundo plano. [33] Desta forma, apenas os investimentos mínimos de sobrevivência para o setor são destinados a área e assim a segurança da informação é tratada como apenas mais uma das diversas atribuições da empresa.

Ratificando, segundo Gil[37], um bom planejamento de segurança é a base para um programa de segurança abrangente e efetivo em relação ao investimento efetuado, entretanto, o principal requisito para o planejamento é o contínuo apoio e participação da alta administração. O planejamento da segurança em informática implica a atuação dos profissionais envolvidos com a tecnologia de informática em atividades dos focos:

- Processos utilizados e de estimativas de resultados esperados – segundo a insegurança estudada;
- Montar/criar possíveis cenários futuros com maiores probabilidades de ocorrências. Deve-se observar também os prováveis resultados visando tanto a segurança preventiva como corretiva, a detectiva e a restauradora;
- Definição visando atividades do setor da informática responsável pela segurança, bem como

para outros usuários, para a segurança patrimonial/empresarial e outros setores da informática;

- Criação de sistemas de informação responsáveis pela captação de indícios e identificação de tendências a situações maliciosas contra a segurança – ai poderão ser buscadas novas práticas de segurança e novas formas de prever situações com elevado poder de desestabilização do sistema de informática;
- Definir situações e simulações que estabelecerão confiança nas medidas de segurança consideradas adequadas;
- Estabelecer objetivos, diretrizes, do perfil, dos custos e do nível do impacto de segurança em informática almejada.

4.2 - Política de Segurança da Informação

Política de Segurança da Informação de uma organização é um conjunto de documentos que descreve quais são os objetivos que todas atividades ligadas a SI (Segurança da Informação) devem trabalhar para atingir. Em linhas gerais, a política resume os princípios de SI que a organização reconhece como sendo importantes e que devem estar presentes no dia-a-dia de suas atividades. A existência desses princípios na política. [37]

Antes de quaisquer exigências quanto a correta utilização dos meios tecnológicos de uma empresa, ou atitudes coerentes segundo processos de proteção a informação, faz-se necessário o estabelecimento de algumas regras, espécies de "leis", que regerão as formas corretas de uso das informações que garantirão a proteção delas. Importante frisar que a existência e a correta utilização e valoramento da Política de Segurança da Informação pela diretoria, presidência, gerência, chefia e alta direção da organização significa uma forma de se exigir aos usuários/funcionários que tais procedimentos sejam seguidos. A existência de uma política deste tipo, que por si só possui disponibilidade a quaisquer funcionários da empresa, exige o conhecimento de todas normas nela contidas não podendo qualquer um destes funcionários alegar não conhecer tais procedimentos.

Dentre outras importâncias, a Política de Segurança da Informação será um ponto crucial na criação de um plano de segurança coeso. Essa será gradualmente implementada, segundo a necessidade e adaptação ao ambiente da instituição servindo como um norteador das atividades,

evitando que funcionários, cada um por si, adotem medidas separadas para prover a segurança. Tudo referente a segurança da informação será cobrado sobre as normas contidas nesta Política de Segurança da Informação e as exigências devem ser cobradas e enquadradas segundo suas normas.

A Política de Segurança da Informação preocupar-se-á com a defesa das informações e sistemas computacionais tanto de software como de hardware de uma empresa assim como se preocupará com o acesso físico e lógico dela. Ela terá também a função de disciplinar o uso destes recursos de forma a padronizar a correta forma de aproveitamento do sistema. Estas atividades necessitarão de controles firmes e podem ser citadas algumas delas:

- Uso correto de software, hardware e equipamentos em geral;
- Gestão de ativos;
- Segurança física e do ambiente;
- Segurança em recursos humanos
- Acesso a rede;
- Acesso a Internet;
- Acesso a informação;
- Gestão de incidentes e continuidade dos negócios;
- Uso de correiro eletrônico;
- Uso de senhas;
- Registro de evidências e eventos (logs);
- Auditorias.

4.3 – Treinamento/educação ao recurso humano

Conforme já citado em dados anteriores, uma pequena porção dos problemas hackers são ocorridos por possíveis ataques. A grande falha provém da falta de treinamento interno e de fragilidades criadas pelos próprios funcionários. Logo um processo de treinamento/educação do recurso humano deve ser realizado. Porém vale destacar que, mais que um simples treino, deve haver a educação dos funcionários e usuários nas possíveis diversas situações.

É necessário o entendimento de que o recurso pessoal precisa alcançar muito além de um treinamento referente a determinado assunto. Para a utilização efetiva e ações numa proteção da informação, deve a pessoa ser/estar educada para tal. Lembrando que a educação para tais procedimentos de segurança exige tanto a prevenção contra algumas ocorrências como a correta forma de se precaver na existência de uma e, mais que isso, como se comportar para reaver as possíveis perdas.

É bom salientar que quando se fala em treinamento, pode-se sugerir que um processo certo e padronizado deva ser seguido visando uma defesa qualificada do sistema. Em outras formas de aprendizagens e qualificações exigidas, um estudo com processos certos e lineares podem ser oferecidos aos pretendentes a conhecer tais conceitos. Na segurança da informação, porém, é proposto um algo mais além de treinamento. A educação do indivíduo é a idéia para um bom aproveitamento e utilização da rede que por si só deve ser entendido como algo mais além de um simples treinamento. Deve-se explorar não apenas o uso de determinados programas, porém a correta utilização de sistemas, modos preventivos, ações que respondam a possíveis ocorrências e até conscientização da forma ideal de explorar os dispositivos de segurança – ou seja, explorar os valores do indivíduo tentando tanto educar quem utilizaria possíveis recursos como quem estaria a entrar no quadro de funcionários locais. O grande diferencial de um treinamento à educação seria exatamente a tentativa de se entender o interior dos usuários do sistema, a tentativa de entender os valores destes associando assim ao treinamento.

Vale destacar que as pessoas têm valores próprios e junto a elas serão estes agregados aos outros valores da instituição. Valores estes herdados inicialmente da família e alterados ao longo da vida. O relacionamento e a relação desta pessoa com a empresa tendem a ser alterados ainda mais com o tempo, tanto estreitando os laços como num possível afastamento de respeito que este funcionário teria com a empresa. Logo, os valores devem ser trabalhados numa gestão da segurança da informação, afinal as pessoas só tendem a valorizar, querer proteger, aquilo que julgam ser importante, que tenham um correto conhecimento da importância e do valor, aquilo que saiba estar protegido por um código de ética da empresa. Mais ainda, a ser enfrentado pela educação, há as vulnerabilidades humanas como a vaidade, a ambição, o medo, a paixão, entusiasmo, etc.

W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale e Don Welch apresentaram trabalho no Workshop da IEEE em Garantia e Segurança da Informação referente ao processo de aprendizado agregando essa ideia de fornecimento de treinamento associado a um processo de educação. [34]

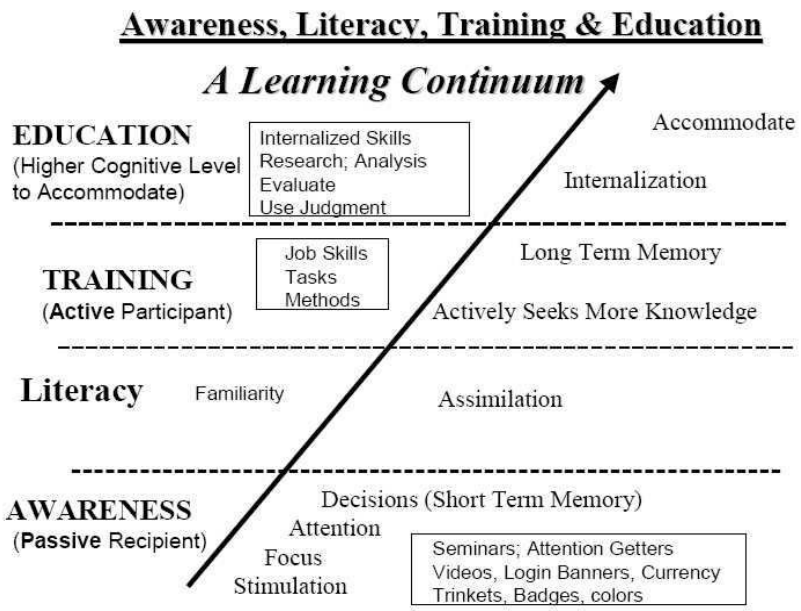


Ilustração 5: Aprendizagem contínua - Maconachy, Schou, Ragsdale e Welch

Este processo de aprendizagem terá quatro fases que são *Awareness* (Conscientização), *Literacy* (Alfabetização), *Training* (Treinamento) e *Education (*Educação). Nesta divisão, serão feitos alguns comentários.

Conscientização

Pessoas devem se conscientizar que fazem parte do problema. Saber que têm função fundamental no processo, pois dificilmente é conseguido algo de alguém que não sabe o que a empresa quer dele num ambiente corporativo e todo processo de aprendizagem deveria começar com essa conscientização [35] .

As pessoas devem saber também se de fato estão cuidando da informação da empresa assim como cuidariam e cuidam das informações com valores pessoais. Ou seja, deve haver uma valorização dos dados da empresa como fossem os seus próprios dados. Devem tomar cuidados básicos que tomariam caso estas informações fossem suas: não abrir alguns links que não abririam em seu computador pessoal, ou deixar de atualizar os sistemas operacionais e softwares em geral.

Acrescentando, a Norma Internacional de Segurança ISO/EIC-17799 tem seção específica nomeada “Conscientização, educação e treinamento em segurança da informação” reforçando a

necessidade de uma conscientização dos usuários.

As pessoas da instituição devem ter a exata noção de que o sucesso da segurança depende muito mais que apenas do setor de segurança da informação. Todos devem ter exata noção que um sistema seguro depende do trabalho de toda instituição e que a importância de cada um é vital para o correto funcionamento conjunto da proteção do sistema. Naturalmente que cada funcionário tem suas atribuições específicas variando as responsabilidades atribuídas e importância técnica no andamento.

Alfabetização

Treinamentos básicos. processos que iriam visar além de treinamentos de programas ou explicações sobre regras de utilização de diversos sistemas. Nesse caso, serão exploradas as utilizações concernentes aos procedimentos internos somadas ao aprendizado dos conceitos da segurança da informação – rede mundial de computadores, vírus, etc. O que há de ser abordado seriam tópicos como o conhecimento da existência de uma Política de Segurança da Informação e o de funcionalidades dos programas de segurança ou procedimentos básicos de defesa.

Os conhecimentos deveriam ser baseados em informações basilares como antivírus, Internet, vírus e seus diversos tipos, formas de ataques, prevenções, engenharia social, perdas causadas por ataques, atualizações a diversos ataques, etc.

Visto que são variáveis as atribuições e responsabilidades, algumas ações na utilização de um sistemas devem ser consideradas básicas por representarem procedimentos corriqueiros e que estas verificações sejam necessárias em quaisquer situações por quaisquer usuários. É importante destacar que todos numa instituição deveriam reconhecer as diversas formas dos seus antivírus representarem os diversos estados deles, se estão funcionando corretamente, se estão atualizados, se estão realmente ativados ou até mesmo se estão instalados alem de tratar estas ocorrências. Sobre estas características, antivírus em geral costumam de alguma forma oferecer informações relacionados aos seus funcionamentos. Outro exemplo é o conhecimento dos funcionários em geral referentes com a atuação em casos de suspeita de ataques. Nada que seja com conteúdo extremamente técnico, porém verificações sobre saber se o antivírus está atualizado, saber como atualizá-lo e a quem informar possíveis ocorrência, mais ainda até mesmo saber o momento de parar a manipulação da máquina em casos de extrema probabilidade delas estarem contaminadas.

Treinamento

A parte correspondente a se aprender, ou seja, aprimorar um conhecimento que já se tem - fazer melhor alguma coisa. Coisa esta que desde antes já se tinha o conhecimento. Ainda para a adaptação às atualizações dos ataques de pragas, é preciso um treinamento visando o tratamento de pequenas variações nas possíveis ocorrências. Na lógica computacional, sempre é necessário que procedimentos comuns sejam seguidos que abordem pequenas variações do ambiente normal – havendo assim informações iniciais ao avaliador da segurança.

Um exemplo poderia ilustrar o que esta fase de treinamento estaria abordando. Depois será comparado este conhecimento com o que seria obtido na fase anterior de alfabetização. O tema será Engenharia Social.

Conhecimento acrescido na Alfabetização:

> A Engenharia Social é uma forma de ataque baseado nas fragilidades humana - técnica esta praticamente descartando-se meios computacionais para o ataque. Tentarão ser exploradas questões como o medo, a insegurança e a confiança do detentor da informação para assim obter informações estratégicas – que as vezes a vítima não tenha ideia de tamanha importância destes dados. As abordagens dos Engenheiros Sociais são baseadas em e-mails, buscas em lixos, tanto físico como virtuais, conversas por fone, conversas pessoalmente dentre outras formas.

Conhecimento acrescido no Treinamento:

1. E-mails com pedidos de possíveis atualizações de dados bancários, dados de cartões, ofertas tentadoras ou premiações consideráveis devem ser vistos de forma cautelosa. Dados bancários, por exemplos, nunca são exigidos por e-mail bem como senhas. Estas ofertas, premiações, são enviadas por algum site que eu estaria cadastrado – teria pedido tais ofertas ou esperaria tais concursos?
2. Nunca devo repassar informações confidenciais, minhas ou da empresa, a quem não conheço ou simplesmente se diz ser alguém com possíveis atribuições e capacidades.
3. Evitar repassar informações muito pessoais em contatos telefônicos sendo esta uma das formas mais comuns de ação destes Engenheiros Sociais. Em qualquer desconfiança de estar sendo vítima de tais golpes, deve-se imediatamente reportar ocorrido ao setor responsável pela segurança da informação bem como aos demais

setores interessados nesses dados.

4. Evitar deixar senhas em geral em papéis de fácil acesso – geralmente ao lado do computador -, ou então simplesmente amassados em lixeiras. Assim como se deve evitar repassar a senha a outras pessoas, mesmo que de sua confiança – afinal estas podem também ser vítimas desta prática.

Educação

Vale ressaltar, como já vimos, que as diversas formas de ataque evoluem e são sempre alteradas – visto isto, percebe-se que sempre haverá uma nova dificuldade para as diversas defesas. O que ocorrerá então? Tentarão explorar novas falhas tanto no aspecto humano como das tecnologias utilizadas. Concluindo, há uma dinâmica na necessidade de aquisição de conhecimentos. Os treinamentos devem ser atualizados visando acompanhar a evolução dos vírus, tanto no ponto de vista tecnológico como treinamentos pessoais. Treinamentos tendem a ficar obsoletos de forma rápida, mais ainda num universo baseado na segurança da informação.

De fato antivírus de grandes empresas têm geralmente consoles centrais que explicam como estão os funcionamentos das diversas máquinas localizadas. Porém o auxílio dos usuários maximizaria na utilização deles além de suprir possíveis falhas na análise causadas por motivos que iriam além da monitoração realizada pelos consoles de antivírus.

Ainda no que fosse abordado sobre treinamento interno, outras citações básicas poderiam ser dadas:

- A existência de uma Política de Segurança da Informação, a importância dela e a obrigação de todos se manterem atualizados;
- Procedimentos básicos de segurança como não acessar certos links com informações suspeitas como promoções exageradas, preços abaixo do mercado, meios fáceis de ganhar dinheiro ou características de códigos maliciosos, material pornográfico, atualizações de dados bancários, receita federal.
- Formas de preocupações com Engenharia Social destacando serem elas as principais formas de ataques na atualidade e a forma de resposta correta a ela, ou seja, reportar a falha ocorrida e dados que facilitem o tratamento dela pelo setor competente.

A verdadeira vantagem do conhecimento dessas ações basilares seria a resolução e até o auxílio ao setor específico pelo tratamento da referida falha.

Vale ressaltar que nesse tipo de treinamento será necessária sempre a reciclagem do conhecimento dos funcionários. Como se sabe, riscos novos tendem a surgir com o passar dos tempos e o aparecimento de novas tecnologias. Logo, uma possível nova infecção generalizada na Rede Mundial de Computadores deve ser seguida de orientação, na forma de treinamento, sobre como lhe dar com as ocorrências bem como saber o valor que a pessoa terá no andamento da segurança do sistema.

4.4 – Procedimentos básicos preventivos de defesa

Algumas dicas simples poderiam ser repassadas visando "boas práticas" de segurança da informação aos usuários do sistema computacional da instituição. Estes procedimentos devem ser resguardados pelo setor de segurança responsável nas questões em que lhe for cabível – escolha e instalação dos softwares, por exemplo, ou atualização dos usuários quanto ao funcionamento às aplicações disponíveis – e tomadas pelo setor as devidas precauções e providências. Conforme percebemos no tópico "Treinamento/educação ao recurso humano", alguns procedimentos básicos devem ser conhecidos e sobre eles ser realizada a educação aos usuários do sistema. Sobre a educação, devemos manter a dinamicidade no conhecimento – procedimento sempre constante de atualização das pessoas sobre as ocasiões.

Apesar da natural tendência de imaginação quanto a segurança da informação numa empresa ser "infalível", deve-se estar atento que todas informações estão sujeitas a ataque e que não há "sistema infalível".

Irrelevante citar que as dicas de segurança são incontáveis e possivelmente estarão desatualizadas um dia após a apresentação deste trabalho – afinal no início dele foi vista a renovação constante na existência de malwares, dos ataques e dos meios de atuação. Estes procedimentos, caso aplicados pelos usuários de um sistemas, são formas que até então cobririam satisfatoriamente as pragas atuais e os exemplos de ataques aqui citados. A atualização destes procedimentos devem ser criados segundo organização do setor específico pela segurança da informação institucional e ciclos de educação devem ser realizados para cada vez mais informar os

usuários de procedimentos de defesa e assim atualizando-os. Estes procedimentos focarão mais o usuário e a prevenção das possíveis falhas humanas.

1. Softwares de segurança:
    - Maximizando a segurança no ponto de vista tecnológico, deve haver antivírus instalados em todas máquinas de um sistema bem como antispywares, firewalls (este será um "paredão" que dividirá a Internet da máquina quanto a troca de informações e seleção sobre o que a rede interna aceitará), antispans, etc;
    - Os programas devem ser de qualidade e reputação conhecida sobre suas capacidades bem como homologados pelo setor de segurança;
    - Deve haver escaneamento de quaisquer arquivos suspeitos pelos respectivos softwares de segurança;
    - Deve o usuário reconhecer o correto funcionamento e procedimentos básicos que estes softwares possam lhe oferecer;
    - Realização de atualizações do antivírus e softwares em geral permitindo o escaneamento realizados temporáriamente por eles ou ativar manualmente o escaneamento. Há uma tendência a pessoa rejeitar os pedidos de atualização ou solicitações de escaneamento do sistema pelo antivírus. Deve considerar estas atualizações e procedimentos como prioridades. Não estando atualizado, evitar, se possível não utilizar, a máquina.
2. Acessos a sites ou links provenientes de e-mails:
    - Não realização de downloads cujo conteúdo venha de sites ou e-mails com reputação duvidosa ou desconhecida;
    - Deve-se checar a fonte das informações recebidas através de e-mails ou sites;
    - Responder as questões: aquela entidade enviou mesmo aquele conteúdo? Ela realiza este procedimento? Eu estou cadastrado ou solicitei dados daquele site?
    - Nunca repassar e-mails ou mensagens quando a integridade e for duvidosa;
    - Não entrar em sites que são notórios redutos de vírus e programas furtadores de senhas, como os pornográficos, downloads de arquivos e jogos gratuitos.
3. Softwares em geral:

- Manutenção de atualização dos softwares da máquina. Os softwares devem estar atualizados contra as possíveis vulnerabilidades.

4. Realizar cópias de segurança periodicamente nos arquivos gerais utilizados.
5. Estar atento a possíveis ataques provenientes de Engenharia Social e conhecer diferentes formas de atuação dos engenheiros sociais.
6. As senhas:
    - Devem ser sempre alteradas;
    - De difícil mapeamento (algo pouco óbvio para um cracker como orrardrdr – iniciais de "O Rato Roeu A Roupa Do Rei De Roma");
    - Uso de caracteres especiais (! @ # $ % &), números, letras maiúsculas e minúsculas;
    - Serem o mínimo repetidas quanto possível nos diferentes serviços utilizados no sistema.
7. Comunicar o ocorrido ao setor de segurança da informação com detalhes do fato em suspeitas de e-mails maliciosos ou de possíveis ataques.
8. Setor de segurança da informação deve sempre comunicar dicas de segurança para a empresa. [36]

4.5 - Segurança Física

Para efetivação de fato da segurança, deve haver um treinamento junto a conscientização sobre o uso e importância das informações envolvidas. Mais que a simples educação da utilização contra falhas virtuais num âmbito digitalizado, deve haver preparação a casos mais complexos, associados a ocorrências cujo ataque se baseie num ataque físico. A Segurança Física é um elemento essencial da Segurança da Informação. É importante notar que não teremos uma Segurança da Informação efetiva sem uma Segurança Física.[33] Investir em diferentes aspectos de segurança sem observar suas devidas prioridades pode ocasionar uma perda de todos os recursos investidos em virtude de uma falha nos sistemas mais vulneráveis.

Desde as áreas de trabalho gerais até àquelas consideradas críticas – como onde ocorrem o processamento de informações confidenciais e críticas -, ou seja, qualquer acesso as dependências da organização, deve haver um controle em que sejam exigidas possíveis formalizações restritivas

aos profissionais autorizados nos respectivos acessos.

Segundo a NBR/ISO 17799, muitas serão às exigências quanto aos requisitos de segurança de terceiros numa empresa – há predominantemente um foco nos contratos quanto a essas negociações na contratação de terceiros. Dentro desses requisitos de segurança será destacada a necessidade de serem inclusos nesses requisitos a segurança física.[23]

A Segurança Física irá atingir todos ativos valiosos ou não da empresa, assim, as preocupações serão muitas e até incontáveis. Alguns exemplos mais comuns dessas preocupações são casos de roubos e furtos; vandalismo e sabotagem; interrupção em serviços básicos como água e energia; terrorismo ideológico; desmoronamento de prédio; enchente, incêndios; etc.

Serão citados alguns mecanismos de proteção físico:

- Proteção de vigias, guaritas, seguranças... – normalmente existente em organizações, deve ser bem definidos os turnos que existirão e quem realizará os procedimentos de defesa bem como a forma correta de procedimentos;
- Acessos aos ambientes – Verificação de identidade da pessoa que adentra ao espaço deve ser realizada. A verificação da aparência humana é importante, porém um controle baseado em biometria, senhas, possíveis identificadores como chaveiros, cartões ou dispositivos a serem lidos por catracas eletrônicas garantem que os acessos são de fato de funcionários que podem estar em tais localizações. Outra forma possível seria de um especialista de fato, com treinamento específico para tal e com alta responsabilidade atribuída a possíveis falhas;
- Circuito Fechado de TV (CFTV) – Sistema que possibilita gravação e acompanhamento em tempo real das movimentações no ambiente. A gravação facilitaria inclusive possíveis processos de perícias e investigações futuras. São diversos os níveis qualitativos de imagem, frequência de captação e até reconhecedores de imagens podendo diferenciar um animal de um ser humano que acabara de ser identificado. Há inclusive captações que facilitam a captura até de traços faciais;
- Sistemas de suporte a abastecimento – Serviços básicos nos fornecimento básicos. Alguns serviços citados poderiam ser os de energia elétrica, água, gás, ventilação, aquecimento, etc.
- Portas e janelas – Ambos são dispositivos que influenciam na segurança física.

Haverá um foco no material que ambos serão construídos e as diversas dificuldades que o material que os compõe ser violado. Estes podem incluir outros recursos que aumentariam a segurança e até acrescentariam outras funcionalidades. Alarme na detecção de quebras ou de acessos a portas de forma indevida – quebra de uma janela ou entrada num ambiente que deveria estar isolado no momento, por exemplo.

- Proteção perimetral – Esta seria a primeira parte da proteção de um espaço perifericamente. Exemplos de proteções são uso de cercas, portões, barreiras estilo "embaixadas". [33]

A proteção dos controles avaliando a educação adquirida deve ser entendida como uma associação às responsabilidades humanas. Serão analisados alguns aspectos relacionados a essa preparação referida.

- Exercícios associados a simulações – Importante frisar que há casos em determinadas cidades onde simulação e exercícios são exigências legais. Este preparo além de ação preventiva, também assume um papel preparatório fundamental. Para efetivação desse treinamento, é importante o envolvimento de todos níveis da organização e todos devem participar demonstrando assim seus comprometimentos. Essa simulação visa uma preparação e a convivência de situações onde poderiam ocorrer casos e desde já adiantar comportamentos falhos e conjuntos que melhorariam a reação às ocorrências.
- Treinamento e conscientização – Deve-se haver uma campanha de conscientização sobre a importância de todos para a garantia da segurança da informação. Não apenas os responsáveis pela segurança da informação deverão ter conhecimentos sobre o processo de defesa, porém todos. Eles próprios devem buscar sempre o repasse dos conhecimentos às outras pessoas, tanto de aspectos que poderiam ser relevante para muitos, como de possíveis palestras atualizando ocorrências. Esse processo de conscientização busca valorizar cada pessoa sobre sua importância atribuindo a elas suas responsabilidades. Ou seja, deve haver uma quebra do paradigma que a segurança da informação tem apenas haver com um setor específico na informática da empresa, que não é nada exteriorizado às outras pessoas. [33]

5 – Conclusão e Trabalho Futuro

Tendo em vista a existência de diversos tipos de ataques realizados, além de novos surgidos diariamente, e do aumento constante na ocorrência deles, é percebida a necessidade de cada vez mais instituições perceberem a segurança da informação como algo estratégico da empresa. Somado a tudo isso, deve-se perceber a importância que a informação tem para uma empresa considerando-a o bem mais precioso que possa haver na instituição.

A importância a ser dada na segurança da informação deve ser vista como prioridade tendo como referência variáveis formas de perdas econômicas ou estratégicas que podem ser percebidas também pela paralisação geral dos serviços corporativos. Nesta precaução, o setor responsável pela segurança deve ter total autonomia na realização de seu trabalho tentando sempre buscar apoio dos diversos setores da empresa. Para isto, deve ser administrada tamanha capacidade conferida ao setor de forma que seja moderada a autonomia dele prevenindo assim possíveis rejeições internas. Sem união, como percebido no trabalho, um sistema tende a ser mais vulnerável.

A implantação de uma segurança qualificada deve ser percebida em três pilares: processos, tecnologia e pessoas sendo a última considerada a mais crítica por especialistas – tanto capazes de deixar maximizar a segurança num sistema como de ser um ponto de vulnerabilidade no acesso aos dados empresariais. Um foco nas pessoas deve ser dado na tentativa de conscientizar acerca de suas importâncias na segurança do sistema e do valor dos dados resguardados. Devem saber que um sistema seguro depende bem mais que apenas do setor de segurança da informação, mas de todos da instituição. Afinal, falhas de pessoas tornam vulneráveis tecnologias ou processos implementados na segurança da instituição.

Em referência a trabalho futuro, uma Política de Segurança da Informação foi percebida como fundamental na implementação de um projeto de segurança. Tantas vezes citada neste trabalho como as “leis”, diretrizes, na implementação da segurança da informação, faz-se necessária uma correta valorização quanto a existência de uma política associada aos procedimentos de sua utilização. É proposta a elaboração de um trabalho que valorize a Política de Segurança da Informação como base para defesa do bem mais importante de uma empresa: a informação.

A ideia seria falar da existência dela em diversas empresas tentando destacar o seu funcionamento e se de fato ela atua como desejado. Mais ainda, poderiam ser realizadas entrevistas as pessoas que a ela devam obediência, assim como os elaboradores, para, nessa comparação de

funcionamento com resposta dos entrevistados, haja uma associação da satisfação extraída pelos usuários com a eficácia aferida dela na empresa. À partir de então, haver um estudo de casos quanto a situação das empresas, as falhas e tópicos que precisam de uma manutenção criando-se uma solução estilo “consultoria” sobre os diversos critérios que a política deveria seguir para melhoria de seu funcionamento. Algumas das análises poderiam ser sobre colaboração da alta administração, auxílio dos diversos setores ajudando na elaboração destas normas, conscientização da importância dela, atualização segundo os costumes da instituição e necessidades atuais, etc. Métricas poderiam ser mensuradas visando sua aplicabilidade na corporação e posteriormente corrigindo as suas precariedades e assim atingindo uma maior abrangência de sua utilização.

6 – Referências Bibliográficas

[1] BALLONI, Antonio José. Porque gestão em sistemas e tecnologias da informação? Revista Unicamp, Campinas, 2002. Disponível em: <http://www.revista.unicamp.br/infotec/artigos/balloni.html>. Acessado em: 5 de abril de 2009.

[2] ---. 10ª Pesquisa Nacional de Segurança da Informação. Módulo *Technology for GRC*. Rio de Janeiro, 2006. Disponível em: http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf. Acessado em: 23 de Abril de 2009.

[3] História: A Evolução do Vírus e Antivírus de Computadores. Disponibilizado em: http://vomicae.net/programas/historia-a-evolucao-do-virus-e-antivirus-de-computador/. Acesso em: 28 de abril de 2009.

[4] Telefônica foi alvo de crackers, avaliam especialistas. Disponível em: http://idgnow.uol.com.br/seguranca/2009/04/09/telefonica-foi-alvo-de-crackers-avaliam-especialistas/. Acesso em: 28 de abril de 2009.

[5] PARKS, Raymon C.; DUGGAN, David P. Principles of Cyber-warfare. Proceedings of the IEEE Workshop on Information Assurance, West Point, NY, p 122 – 125, 2001. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2001, West Point, NY.

[6] Alemanha treina hackers para guerra do futuro. Disponível em: http://tecnologia.terra.com.br/interna/0,,OI3514439-EI4805,00-Alemanha+treina+hackers+para+guerra+do+futuro.html. Acesso em: 7 de maio de 2009.

[7] Virus - A category with broad experience which keeps out of the new malware dynamic. Disponível em: http://www.pandasecurity.com/homeusers/security-info/classic-malware/virus/?

sitepanda=particulares. Acesso em: 8 de maio de 2009.

[8] Denial of Service Attacks. Disponível em: http://www.cert.org/tech_tips/denial_of_service.html. Acesso em: 8 de maio de 2009.

[9] Keylloger. Disponível em: http://pt.wikipedia.org/wiki/Keylogger. Acesso em: 15 de maio de 2009.

[10] Vírus interrompe Serviços prestados pelo DETRAN em Pernambuco. Disponível em: http://g1.globo.com/Noticias/Brasil/0,,MUL990097-5598,00.html. Acesso em 10 de abril de 2009.

[11] SCHNEIER, Bruce. *Thwarting an Internal Hacker.* Disponível em: http://online.wsj.com/article/SB123447990459779609.html. Acesso em 10 de abril de 2009.

[12] *Government Hack Attacks Prompt Scrutiny.* Disponível em: http://blogs.wsj.com/digits/2009/02/16/government-hack-attacks-prompt-scrutiny/?mod=rss_WSJBlog?mod=. Acesso em: 12 de abril de 2009.

[13] *The Spread of the Sapphire/Slammer Worm.* Disponível em: http://www.caida.org/publications/papers/2003/sapphire/sapphire.html. Acesso em: 13 de abril de 2009.

[14] *The weakest security link? It's you*. Disponível em: http://news.cnet.com/2100-7355_3-5278576.html. Acesso em: 13 de Abril de 2009.

[15] Hacker regenerado. Disponível em: http://infoaux-security.blogspot.com/2009/03/hacker-regenerado.html. Acesso em: 03 de maio de 2009.

[16] MITNICK, Kevin David e SIMON, William L. A Arte de Enganar – Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Ed. Pearson, 2003.

[17] Conheça os 8 erros de segurança que os usuários mais cometem nas empresas. Disponível em: http://idgnow.uol.com.br/seguranca/2009/01/16/conheca-os-8-erros-de-seguranca-que-os-usuarios-mais-cometem-nas-empresas/paginador/pagina_4. Acesso em 20 de abril de 2009.

[18] GORDON, L. A.; RICHARDSON, R. The new economics of information security. Information Week, n. 982, p. 53–56, Mar. 2004.

[19] SCHNEIER, B. Secrets and Lies: digital security in a networked world. New York: John Wiley & Sons, 2000.

[20] *The human firewall*. Disponível em: http://www.networkworld.com/research/2003/0526human.html. Acesso em: 16 de abril de 2009.

[21] Um terço dos internautas usa a mesma senha para todos os sites. Disponível em: http://wnews.uol.com.br/site/noticias/materia.php?id_secao=1&id_conteudo=12874. Acesso em: 18 de maio de 2009.

[22] Dez falhas em Segurança da Informação! Disponível em: http://penguim.wordpress.com/2009/05/14/dez-falhas-em-seguranca-da-informacao/. Acesso em: 14 de maio de 2009.

[23] PEIXOTO, Mário César Pintaudi. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport, 2006.

[24] MITNICK, Kevin D.; SIMON, William L. A arte de enganar – Ataques de hackers: controlando o fator humano na segurança da informação. *Pearson Education.* São Paulo, 2003.

[25] CUNHA, Roberto. *Treinando Macacos e Educando Pessoas*. Belo Horizonte, 2007. Monografia (MBA em Gerência de Telecomunicações) – Fundação Getúlio Vargas.

[26] Pesquisa: 59% dos ex-funcionários desviam dados corporativos. Disponível em: http://idgnow.uol.com.br/seguranca/2009/02/25/pesquisa-revela-que-59-dos-ex-funcionarios-desviam-dados-corporativos/. Acesso em: 16 de abril de 2009.

[27] ALMEIDA Junior, J. R.; Segurança em Sistemas Críticos e em Sistemas de Informação – Um estudo Comparativo. Tese de Livre Docência. Escola Politécnica da USP, 2003.

[28] Pesquisa realizada pela Revista Veja com título "A ESCALA DO RISCO DIGITAL – De 1 a 10, o grau de perigo causado por certos procedimentos ao computador" com os especialistas Eduardo Marques, Carlos Almeida Jr. E Jecel Assumpção Jr./ICMC-USP; Alexandre Freire (UFRJ, autor de Como Blindar Seu PC); Hélio Guardia (UFSCar); Adriano Cansian (Unesp) na edição 2113 – ano 42 – nº 20. Data: 20 de maio de 2009.

[29] May Headline: Programming language D suffers sharp fall. Disponível em: http://www.tiobe.com/index.php/content/paperinfo/tpci/index.html. Acesso em: 13 de mais de 2009.

[30] WANG, H.; WANG, C. Taxonomy of security considerations and software quality: addressing security threats and risks through software quality design factors. Communications of the ACM, v. 46, n. 6, p. 75–78, June 2003.

[31] TRYFONAS, T.; KIOUNTOUZIS, E.; POULYMENAKOU, A. Embedding security practices in contemporary information systems development approaches. Information Management & Computer Security, v. 9, n. 4, p. 183–197, 2001.

[32] Segurança da informação. Disponível em: http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o. Acesso em: 18 de maio de 2009.

[33] Security Officer – 1: guia oficial para formação de gestores em segurança da informação / Anderson Ramos (org.); Porto Alegre, RS: Zouk, 2006. (Módulo Security Solutions).

[34] " A Model for Information Assurance: An Integrated Approach", publicado em "Proceedings of the 2001 IEEE Workshop on Information Assurance and Security" e disponível em

http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2C3(55).pdf

[35] Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil 2005 Disponível em: <www.nic.br/indicadores.pdf> Acesso em 18 de maio de 2009.

[36] "Não há Limites para o Crime Virtual". Entrevista de Kevin Mitnick à Revista Veja, nº 20, ano 42, edição 2113. 20 de maio de 2009.

[37] GIL, Antonio de Loureiro. Segurança em informática. 2. ed. São Paulo: Atlas, 1998. 192 p.

[38] Hackers entram na rede elétrica dos EUA, diz jornal. Disponível em: http://tecnologia.terra.com.br/interna/0,,OI3691785-EI4805,00-Hackers+entram+na+rede+eletrica+dos+EUA+diz+jornal.html. Acesso em: 02 de maio de 2009.

APÊNDICE A – Glossário

Serão destacados alguns termos atinentes a Tecnologia da Informação (ou Informática), maior foco às referências a segurança da informação, que foram citados neste trabalho. Entretanto uma maior explicação momentânea até então se fazia desnecessária visando o objetivo específico deste projeto.

Antivírus

Softwares projetados para detectar, eliminar e realizar tratamentos em geral sobre vírus de computador.

Antispyware

Programas utilizados para combater, entre outros malwares, spywares. Há programas com essa função específico e outros com esta função incluída como firewalls e antivírus.

Assinatura Digital

Mecanismo que identifica o remetente de mensagem eletrônica. Esta técnica comprova que tal documento foi enviado pela pessoa que diz ter enviado. Uma segurança ao receptor da mensagem.

Cracker

Prática a quebra de sistema de segurança de forma ilegal e sem quaisquer éticas. Criado em defesa da palavra “hacker” que erroneamente era utilizada quando designadas essas ações criminosas, porém hoje continua essa confusão quanto ao uso da expressão. Algumas atuações são a quebra de softwares pagos para utilização deles de forma gratuita, quebra de criptografias ou senhas e desenvolvimento de malwares.

Criptografia

Mensagem escrita em códigos, numa linguagem desconhecida para todos, exceto para uma outra

ferramenta tradutora específica para a situação. Na informação serão aplicadas técnicas e ferramentas que transformarão a mensagem original numa outra ilegível de forma a ser reconhecida apenas pelo receptor. Este terá um mecanismo para tradução da mensagem criptografada.

Extensão ".exe"

Extensão executada em computadores com sistema operacional Windows e DOS. Quando executadas, representam uma autorização do usuário para execução daquele programa – portanto, sem maiores cuidados, através dele, pode-se instalar um vírus de computador.

Firewall

Dispositivo de rede de computadores que aplica uma política de segurança num determinado ponto de rede. Regula tráfego de informações entre redes distintas impedindo transmissão ou recepção de acessos nocivos entre as redes.

Hacker

Mais considerado como o "decifrador de códigos". Objetivam a modificação de programas de computador acrescentando funcionalidades diferentes da original. A modificação deles busca tentar melhoria de programas atendendo a legalidade nas modificações. Um exemplo de hackers são as pessoas que fizeram as modificações do linux para o estágio que hoje se encontra o sistema operacional.

Hardware

Parte física do computador. Conjunto de componentes eletrônicos, circuitos integrados e placas se comunicando através de barramentos.

IDS

Sistema de detecção de intrusos (do inglês "Intrusion detection system"). O IDS realiza a indicação de ações crackers em redes bem como atuações má intencionadas em geral.

IP

Proveniente do inglês “Internet Protocol”. Protocolo, regras de conversação entre duas máquinas, para troca de informação entre duas máquinas.

Malware

Proveniente do inglês (Mal vem de “**mal**icious”; Ware, “soft**ware**”). A tradução quer dizer programa malicioso. Este é destinado a se infiltrar num sistema alheio de forma ilícita visando roubo de informação ou causar danos na máquina. Vírus, trojans, worms e spywares são exemplos.

Rede de Computadores

Dois ou mais computadores conectados entre si, podendo haver mais dispositivos além de apenas computadores. Visa o compartilhamento de serviços como troca de dados, mensagens, impressoras, Internet, etc.

Software

Programas de computadores. Parte lógica do computador. Instruções lógicas escritas numa linguagem de programação para realizarem um determinado serviço no computador, uma função a ser executada num hardware aproveitando sua utilidade.

Spam

Mensagem eletrônica não solicitada enviada em massa. Normalmente realiza função de divulgações publicitárias com caráter incômodo e incoveniente.

Spyware

Programa espião que recolhe informações sobre o usuário, principalmente seus costumes em sites para enviar estas informações a uma unidade externa dessa máquina. O spyware atua enviando estas informações sem quaisquer consentimentos do usuário, pode tanto ser desenvolvido por firmas comerciais em busca de informações de navegação, como pode ser desenvolvido por criminosos a fim de conhecer mais sua possível “vítima”, fragilidades dela ou obtenção de dados bancários.