UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA EM COMPUTAÇÃO
FERNANDA MONTEIRO SARAIVA

UM ESTUDO PRÁTICO SOBRE SEGURANÇA DA INFORMAÇÃO

PATOS
2012

FERNANDA MONTEIRO SARAIVA

UM ESTUDO PRÁTICO SOBRE SEGURANÇA DA INFORMAÇÃO

Monografia de graduação apresentada ao Departamento de Licenciatura em Ciência da Computação da Universidade Estadual da Paraíba como parte das exigências do curso de Licenciatura em Computação para obtenção do título de Licenciado em Computação.

Orientadora: Profª. Msc. Jannayna Domingues Barros Filgueira

PATOS

2012

S243e Saraiva, Fernanda Monteiro

Um estudo prático sobre segurança da informação/ Fernanda Monteiro Saraiva. Patos: UEPB, 2012.

60f. : il.

Trabalho de Conclusão de Curso (Licenciatura em Ciência da Computação)–Universidade Estadual da Paraíba. Orientadora: Prof.ª Msc. Jannayna Domingues Barros Filgueira.

1. Redes de computadores – Medidas de Segurança. 2. Segurança de computadores. I. Título. II. Saraiva, Fernanda Monteiro.

UEPB/SIB/Setorial - Campus VII CDD 005.8

UNIVERSIDADE ESTADUAL DA PARAIBA
DEPARTAMENTO DE COMPUTAÇÃO

CERTIFICADO DE APROVAÇÃO

Um Estudo Prático Sobre Segurança da Informação

Autora: Fernanda Monteiro Saraiva

Orientador: Profª. Msc. Jannayna Domingues Barros Filgueira

Aprovada em 03 /12 / 2012

BANCA EXAMINADORA:

Jannayna Domingues Barros

Jannayna Domingues Barros

(Orientadora)

Ana Isabella Muniz Leite

Ana Isabella Muniz Leite

Tatiana Cristina Vasconceios

Dedico este trabalho primeiramente a Deus, por ter me dado esta oportunidade de estudar e concluir minha graduação, sem a sua grande ajuda, motivação e força de vontade jamais iria chegar até o final, ao meu pai Saraiva, minhas irmãs pelo grande apoio nesta jornada e a todos os meus amigos que indiretamente contribuíram para minha vitória.

AGRADECIMENTOS

Concluir uma graduação é uma importante meta alcançada por um ser humano, é um passo dado para a obtenção de um objetivo, por isso agradeço sempre a Deus por colocar importantes desafios em meu caminho e por sempre testar minha capacidade de concluir algo.

A toda minha família, principalmente ao meu pai, José Saraiva Correia Filho por ter me iniciado na área de informática, tendo me incentivado e ajudado sempre que necessário.

A minha orientadora, Profª. Jannayna por toda dedicação nas etapas deste trabalho.

Aos meus amigos que me incentivaram e sempre me deram força para que eu pudesse vencer esse desafio.

A todos os professores do curso de computação da UEPB que foram fundamentais para o meu aprendizado e formação profissional.

A todos os colegas de sala que sempre compartilharam comigo meus momentos de estresse e muitas risadas.

“A persistência é o caminho do êxito”.
Charles Chaplin

SARAIVA, Monteiro Fernanda. Segurança da Informação: Um estudo de Caso. Trabalho de Conclusão de Curso. Curso de Licenciatura em Computação. Universidade Estadual da Paraíba. Patos - PB, 2012. 66 f.

RESUMO

O presente trabalho traz uma análise sobre os perigos que a tecnologia pode vir a sofrer com ataques de hackers que tentam obter informações sigilosas de sistemas de empresas ou de um computador pessoal. A informação passou a ser um ativo cada vez mais valorizado pelas organizações e governos, onde prevalece o uso da tecnologia da informação fazendo com que os dados e o conhecimento sejam disseminados numa rapidez jamais imaginada, sendo assim indispensável para as empresas o investimento em Segurança da Informação. Manter a esta significa preservar sua confiabilidade, integridade e disponibilidade. Partindo destes princípios, serão expostos ferramentas e métodos essenciais que auxiliam na prevenção da segurança da informação no mundo moderno. Este estudo monográfico produz uma análise prática realizada na empresa SOLNET localizada na cidade de Patos – PB. Serão mostradas e avaliadas as práticas da Segurança da Informação da mesma. Foi realizada uma coleta de dados baseada em um questionário estruturado com perguntas fechadas. Constatou-se que a informação é preciosa e fundamental e que os entraves para maiores investimentos é de ordem orçamentária.

Palavras-chave: Tecnologia, Segurança da Informação, Hacker.

SARAIVA, Fernanda Monteiro. Information Security: A Case Study. Completion of Course Work. Degree in Computing. Universidade Estadual da Paraíba. Patos - PB, 2012. 66 p.

ABSTRACT

This paper presents an analysis of the dangers that technology might suffer attacks from hackers who somehow try to get sensitive information from business systems or a personal computer. The information has become an increasingly valued asset for governments and organizations, where prevails the use of information technology so that data and knowledge are disseminated in a speed never imagined being so indispensable to business investment in information security. Maintaining information security means preserving its confidentiality, integrity and availability. Based on these principles, tools and methods will be exposed essential that aid in the prevention of information security in the modern world. This monographic study makes a case study conducted in SOLNET company located in the city of Patos - PB. Will be shown and evaluated the practices of Information Security the same. We performed a data collection based on a structured questionnaire with closed questions. It was found that the information is valuable and important and that the barriers to greater investment is of a budget.

Keywords: Technology, Information Security, Hacker

LISTA DE SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

DNS - Domain Name Service

FTP - File Transfer Protocol

IP - Internet Protocol

ISO - International Standards Organization

PC - Personal Computer

TCC - Trabalho de Conclusão de Curso

TCP - Transmission Control Protocol

TI - Tecnologia da Informação

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

A globalização veio comportar a mundialização das novas tecnologias oferecendo assim oportunidades a todos, com o espaço geográfico fragmentado, porém intensamente articulado pelas redes, em que a informação, independente do seu formato, é um dos maiores patrimônios de uma organização moderna, sendo fundamental para qualquer nível hierárquico dentro de uma instituição que deseja manter-se competitiva no mercado.

Com o crescimento da informática, o mundo tornou-se cada vez mais interligado e as informações passaram a ser instantâneas. Essa globalização causou a necessidade do desenvolvimento de inovações tecnológicas, possibilitando assim realizar diferentes funcionalidades para facilitar o trabalho desenvolvido nas empresas e o contato da mesma com o público externo. Entretanto, tais facilidades podem levar os computadores a vulnerabilidades e ameaças. Para impedir tais exposições, surge a Segurança da Informação.

De acordo com Soares (1995) o termo segurança é usado com o significado de minimizar ameaças a bens e recursos. No mundo tecnológico, os riscos e ameaças a segurança representam para redes e sistemas um fator de alta preocupação quando se trata de vulnerabilidade a que está exposta pessoas e empresas. Vulnerabilidade é uma fraqueza que pode ser explorada para se violar um sistema ou informação que ele contém (FREITAS, 2006).

A informação, tem se tornado um dos recursos mais importantes no mundo dos negócios. Nesse panorama de globalização e competição, é percebível a existência de duas forças antagônicas: de um lado, as empresas que lutam para manter suas informações protegidas, em especial as consideradas estratégicas e de outro lado, os invasores que motivados por diversos fatores, objetivam captar estas informações. É neste contexto que a Segurança da Informação opera, na tentativa de evitar invasões e vazamentos de informações, ou ao menos abrandar os prejuízos decorrentes dos mesmos.

A Segurança da Informação tem como objetivo garantir que a empresa fique protegida contra as possíveis ameaças externas e internas que possam originar impacto ao funcionamento habitual dos negócios (SÊMOLA, 2003). Com isso, os investimentos em Segurança da Informação precisam ser conduzidos com a mesma seriedade com a qual os administradores decidem expandir sua linha de produção ou automatizar sua força de vendas, ou seja, pensando no retorno sobre esse investimento. As empresas que não se preocupam com Segurança da Informação, cultivam falhas que degradam a confidencialidade, integridade

e disponibilidade dos seus sistemas, arquivos e servidores facilitando assim o risco de sofrer um simples ataque até uma indisponibilidade completa de seus sistemas gerenciais.

Com o aumento das atividades on-line a segurança precisa adequar-se aos novos tempos para fornecer facilidades de uso seguro e assumir o uso mais responsável da tecnologia, comprometendo-se com sua integridade digital. A Segurança da Informação não é apenas uma atitude, uma pessoa ou um produto, são modelos que se implementados em conjunto vão garantir a segurança das redes e da informação nas empresas.

As técnicas e os métodos de proteção à informação são variados e mudam de acordo com a evolução das ameaças, mas podemos definir algumas medidas e ferramentas básicas para a segurança de ambientes computacionais, como manter o sistema operacional atualizado, efetuar backups dos arquivos, usar antivírus e implementar um firewall. Entretanto, quando se pensa em medidas para a proteção dos recursos computacionais, deve haver um compromisso entre a funcionalidade e a segurança.

1.1 OBJETIVO GERAL

Segurança é um assunto muito amplo, principalmente se for levado em importância a grande variedade de problemas que poderão estar incluídos ao tema. Dentro desta ótica, este trabalho mostrar o atual valor da informação, a necessidade do uso das tecnologias da informação, a importância com a Segurança da Informação e quais os principais recursos para uma assertiva Segurança da Informação dentro de uma empresa.

1.2 OBJETIVOS ESPECIFICOS

Para alcançar o objetivo geral, foram propostos os seguintes objetivos específicos:

– Estudar os elementos de Segurança da Informação, no âmbito físico, tecnológico e humano;

– Analisar a importância da Segurança das Informações para os profissionais;

– Estudar sobre algumas técnicas utilizadas pelos invasores;

– Analisar a Políticas de Segurança da Informação do provedor de internet SOLNET.

1.3 JUSTIFICATIVA

Segurança da Informação é assunto de debate para as corporações que buscam saídas práticas e efetivas para aperfeiçoar suas atividades e garantir segurança nos seus mecanismos de trabalho. A forma como as empresas devem administrar este desafio, se apresenta sob aspectos de ordem tecnológica e de ordem humana. Assim se faz necessário para qualquer organização a criação de uma política de segurança formal, clara e objetiva, visando à Segurança da Informação com foco nas informações trocadas pela mesma.

1.4 METODOLOGIA

Foram realizadas pesquisas em livros e sites especializados que contribuíram para delinear um quadro teórico e um levantamento preliminar de alguns problemas que podem ocorrer quando o assunto tratado é Segurança da Informação.

Esta monografia apresenta uma pesquisa exploratória e foi desenvolvida com uma metodologia baseada nas etapas apresentadas a seguir: inicialmente foi feita uma pesquisa bibliográfica sobre os temas Segurança da Informação e qualidade da informação como produto. Em termos metodológicos, este trabalho enquadra-se dentro da tipologia de uma análise prática onde, a partir da descrição de um caso particular da empresa SOLNET, se procurou responder os objetivos traçados. Para o recolhimento dos dados realizou-se uma pesquisa fundamentada na técnica de entrevista direcionada ao responsável pela área das redes de comunicações e Segurança da Informação da empresa.

Como etapa seguinte foi feita uma coleta de dados na corporação, para uma analise posterior a partir dos resultados obtidos. Devido à complexibilidade de se aprofundar em todos os aspectos relacionados à Segurança da Informação em um único trabalho, a proposta desenvolvida nessa monografia visa percorrer os fundamentos da Segurança da Informação aprofundando-se no questionário aplicado, entrevista e analise de resultados obtidos da instituição a qual foi realizada a análise prática: A SOLNET.

Este trabalho foi organizado em sete partes, estando os iniciais voltados à fundamentação teórica necessária e os posteriores às atividades efetivamente desenvolvidas.

No Capítulo 2, será introduzido um breve histórico sobre o desenvolvimento das redes de computadores e da computação. Serão abordados os principais tópicos relacionados à Segurança da Informação, como os conceitos básicos de segurança, informação e a importância das mesmas.

No Capítulo 3, discutisse-se a questão de vulnerabilidade e ameaças do sistema, os tipos de invasores e as principais técnicas de invasão.

O Capítulo 4 fornece uma visão geral sobre os mecanismos de segurança e passa-se a discutir sobre as ferramentas para detecção de vulnerabilidades.

O Capítulo 5 apresenta sobre as políticas de segurança as normas e padrões que orientam a área de Segurança da Informação.

Para avaliação e verificação o capítulo 6 trás um estudo prático. Apresentando os problemas relacionados à vulnerabilidade, serão mostradas e avaliadas as práticas da Segurança da Informação da empresa SOLNET fazendo uma revisão dos argumentos apresentados e mostrando os resultados obtidos pelo estudo prático proposto e coloca o trabalho como sendo uma fonte para os interessados no assunto de segurança da informação e suas características dentro da computação.

O último capítulo é apresentado à conclusão do trabalho onde é abordada a confirmação das hipóteses levantadas.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 INTRODUÇÃO A REDES DE COMPUTADORES E INTERNET

Os seres humanos perceberam, desde o início da humanidade, que a sua sobrevivência dependia da comunicação. A partir dai os homens buscam aperfeiçoar os sistemas de comunicação. A todo instante as pessoas se deparam com algum computador ou terminal de rede, nos caixas automáticos dos bancos, nos terminais das lojas, na sua casa, nas academias, bares... As redes de computadores estão em todas as partes. Talvez a Internet venha a ser a 3ª maior rede do mundo, em termos de abrangência, perdendo apenas para as redes elétrica e telefônica.

Uma rede de computadores é a conexão de dois ou mais computadores para permitir o compartilhamento de recursos e a troca de informações entre as máquinas (TANENBAUM, 2003). Uma rede pode ser composta por vários sistemas operacionais, e por dispositivos de diferentes fabricantes. Pode ter vários tamanhos e abrangências, bem como formatos físicos distintos. A Internet é um amplo sistema de comunicação que conecta várias redes de computadores (SANTOS 2005). Existem muitas formas e vários equipamentos que podem ser interligados e compartilhados, por meios de acesso, protocolos e requisitos de segurança.

As redes de computadores são o núcleo da comunicação moderna e essa explosão, nas comunicações, não teria sido possível sem o avanço constante dessa tecnologia. A partir do momento em que os computadores passam a transmitir dados na rede, eles passam também a ter alguns problemas de segurança, pois quando muitas pessoas acessam informações são necessários cuidados para que não haja acessos impróprios da mesma.

Devido ao grande aumento dos problemas relacionados à segurança, as empresas estão começando a investir mais nesta questão. A Segurança da Informação não é apenas uma atitude, uma pessoa ou um produto, são várias atitudes que em conjunto vão garantir a segurança das redes de computadores nas empresas.

2.2 INFORMAÇÃO

Segundo Dias (2000), a informação é o principal patrimônio da empresa e está sob constante risco. A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, transmitida pelo correio ou por meios eletrônicos, mostrada em filmes ou

falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente (NBR ISO/IEC 17799, 2001).

Segundo a ABNT NBR ISO/IEC 27002 (2007), a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida.

Sêmola (2003) define como informação:

> Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos ou transacionais. A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvos de proteção da segurança da informação.

2.3 CONCEITOS BÁSICOS DE SEGURANÇA

O uso de computadores vem crescendo muito rápido, devido a isso, o interesse das pessoas em saber mais sobre este assunto e buscar informações no ambiente virtual vem crescendo proporcionalmente.

Quando muitas pessoas acessam informações é indispensável que haja certo cuidado para que não exista acesso de pessoas não autorizadas a esses dados. A realidade é que nenhum sistema é totalmente seguro, o que se tem são várias medidas de segurança que se implementadas em conjunto podem diminuir tais problemas.

A Segurança da Informação tem como objetivo básico proteger os dados que trafegam para assim garantir a sua confidencialidade, a sua integridade e a sua disponibilidade:

Confidencialidade: O controle de autenticidade está associado com identificação de um utilizador ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital.

Integridade: É a propriedade que garante a chegada de certa informação ao seu destino de uma maneira integra, sem que ela tenha passado por nenhuma mudança em seu conteúdo em algum período de sua existência.

Disponibilidade: A disponibilidade consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao utilizador o acesso aos dados sempre que deles precisar.

Com toda essa tecnologia que nos rodeia, há a necessidade que usuários de computadores e as pessoas que trabalham diretamente com a segurança da informação fiquem atentos as inovações tecnológicas, estando continuamente atualizados para que contra tempos sejam evitados. Esse avanço tecnológico também traz sérias consequências no ambiente coorporativo que precisam ser avaliadas e abordadas. Os problemas catalogados com a Segurança da Informação são produtos dessa própria evolução, que possibilita a integração cada vez maior de ambientes de redes distintas que se tornam cada vez mais complexas.

2.4 A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Vários assuntos devem ser avaliados quando uma rede passa a compor parte importante da organização. Recentemente, devido à utilização do uso da Internet nas empresas e a importância da informação como estratégia, aparece à necessidade de um maior e melhor domínio sobre informações sigilosas e um crescente interesse de pessoas maliciosas em obter acesso não autorizado. Vários especialistas creem que com a rápida evolução tecnológica, nenhum ambiente é totalmente seguro, para minimizar os riscos de ataques, diversas tecnologias devem ser empregadas.

A Internet está se concretizando como uma nova forma das pessoas fazerem negócios. Algumas empresas só disponibilizam seus produtos pela Internet. É cada vez mais frequente o uso da informação alinhada à tática de uma empresa, a fim de lhe trazer benefícios e vantagens. Isso ocorre através da divulgação de seus produtos, promovendo a inovação e diminuindo os custos do negócio.

A Segurança da Informação é um fator primordial na tomada de decisões e nos investimentos das empresas, tornando-se parte do próprio negócio. Grande parte das empresas tem orçamento específico para a área de tecnologia da informação e para área de segurança. Porém ainda existem algumas empresas que deixam a segurança em segundo plano, dando-lhe a devida importância apenas quando são invadidas e suas informações roubadas. Não recebendo a devida importância e sem a definição de uma boa estratégia de segurança, são utilizadas técnicas parciais ou incompletas que podem aumentar a vulnerabilidade da organização (NAKAMURA, 2003).

Nas empresas, seus sistemas de informação são sujeitos a diversos tipos de ameaças incluindo fraudes eletrônicas, vandalismo, espionagem e sabotagem. Danos causados por códigos maliciosos e crackers estão se tornando cada vez mais comuns, mais ambiciosos e inacreditavelmente mais sofisticados.

Segundo MEDEIROS (2003) a importância da informação, além de estar focada em sua aquisição, passou a ser definida também pelo tempo que uma empresa leva para adquirir, processar e transformar a informação.

3 CONSIDERAÇÕES SOBRE SEGURANÇA

3.1 VULNERABILIDADES, AMEAÇAS E ATAQUES

Anteriormente as empresas davam importância apenas para a questão financeira e para o patrimônio. Essa visão tem mudado levando-as a assumirem que a informação é essencial para a conservação dos negócios. Para proteger os bens de uma organização é preciso compreender contra o que se estará protegendo, quais os riscos e ameaças existentes.

Os desafios para implementar um modelo de segurança envolve aspectos tecnológicos, físicos e humanos do ambiente de negócios de uma empresa e por esse motivo se faz necessário a identificação da situação de segurança, fazendo um levantamento das vulnerabilidades e prioridades de proteção. As vulnerabilidades são desencadeadas de costume intencional ou por acontecimento acidental.

Para um melhor entendimento segue abaixo a definição de vulnerabilidade, ameaça e ataque.

Vulnerabilidade**:** Um ponto fraco na segurança do sistema que pode ser explorada por invasores com diferentes interesses. As vulnerabilidades por si não provocam incidentes, elas são apenas possibilidades de exploração por um agente causador, de forma intencional ou não. Segundo Oliveira (2004), os tipos de vulnerabilidades são:

- Físicas: Instalações prediais fora do padrão; riscos de explosões ou incêndios; controle de acesso precário às instalações;
- Naturais: Computadores que guardam as informações importantes são susceptíveis a desastres naturais, acúmulo de poeira nos barramentos de comunicação da placa-mãe que pode causar falhas nos sistemas;
- Software: Possíveis erros na configuração ou na própria instalação podem acarretar acessos indevidos;
- Humanas: As ações humanas também podem acarretar certas vulnerabilidades, como a falta de treinamento em segurança que faz com que muitos funcionários sejam alvos em potencial de um ataque de engenharia social. Outros exemplos também podem ser observados como sabotagens, vandalismo e roubo.

Como exemplo de uma vulnerabilidade pode-se citar os computadores da organização que não possuem as ultimas definições do banco de dados de vírus para o software anti-malware.

Ameaça**:** Quem ou o que pode atacar um componente, usando uma ferramenta ou recurso. Qualquer evento que possa causar dano a um sistema ou rede. Por definição, a ameaça seria um possível agente explorador de uma vulnerabilidade. Segundo Oliveira (2004), os tipos de ameaça são:

- Naturais: São ameaças provenientes dos fenômenos da natureza como enchentes e terremotos.
- Voluntárias: São causadas por seres humanos como hackers e disseminadores de vírus.
- Involuntárias: São causadas, quase na totalidade das vezes, por desconhecimento. Podem ser causadas por erros.

Ataque**:** Uma tentativa de causar danos a ativos valiosos, tentando explorar as vulnerabilidades. O dano pode incluir roubo de informações, destruição, espionagem, adulteração entre outros (SILVA, 2007).

3.2 TIPOS DE INVASORES

Segundo Erick S. Raymond (2003), em Informática, hacker é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. Graças a esses conhecimentos, um hacker consegue obter soluções e efeitos extraordinários, que extrapolam os limites do funcionamento comum dos sistemas, como previstos pelos seus criadores incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controle de sistemas e acesso a dados. De acordo com os hackers, crackers são elementos humanos que invadem sistemas para furtar informações deixando para trás um rastro de estragos que trazem problemas às vítimas.

O termo cracker é uma designação empregada para aqueles que decodificam códigos e destroem as proteções do software. Existe também o cracker de senha. Este por sua vez é um elemento que se aproveita de um determinado software avançado para descobrir senhas ou interpretar mensagens cifradas. Os invasores são programadores habilidosos, dominam mais de uma linguagem de programação. Muitos são jovens, especialmente estudantes (desde nível

médio a pós-graduação). Possuem conhecimentos aprofundados sobre ferramentas, serviços e protocolos e também grande experiência com Internet. Por se dedicarem muito tempo a pesquisa e experimentação, hackers/crackers tendem a ter reduzida atividade social e se encaixar no estereótipo do nerd. Conhecem verdadeiramente pelo menos dois sistemas operacionais.

Logo abaixo serão definidos alguns tipos de invasores segundo Dumont (2006):

Lamer: É aquele que deseja aprender sobre hackers, e está sempre fazendo perguntas a todos. É um pseudo-hacker ou pseudo-cracker. Sem conhecimentos técnicos de qualquer ordem para atacar a segurança informática de uma organização, sistema ou rede. No entanto, usa programas ou partes de programas disponíveis na Internet para efetuar os seus ataques.

Script Kiddie: Não possuem muita habilidade, é alguém que procura por um alvo fácil. Este alguém não procura por informações específicas, o seu objetivo é obter acesso à conta de usuários da maneira mais simples possível. Já encontram a informação para a possível invasão pronta na internet e com sorte o sistema não aplicou o patch de correção a tempo.

Cracker: Agem para prejudicar financeiramente alguém ou em benefício próprio, suas atitudes furtivas poderão enganar até aos mais experientes administradores, são os verdadeiros invasores, criminosos cibernéticos.

Hacker: Não usa de más intenções. Tenta oferecer um serviço à comunidade interessada. Não são fúteis desconfiguradores de páginas. São Programadores ou administradores de rede que se reservam a questionar os problemas de segurança nas tecnologias disponíveis. Exemplos: Linus Torvalds, Ada Lovelace, Douglas Engelbart, Dennis Ritchie, Ken Thompson, Arnaldo Melo, Marcelo Tossat, Alan Cox.

Phracker: São especializados em telefonia, suas principais atividades se baseiam em ligações gratuitas, reprogramação de centrais telefônicas e instalação de escutas.

3.3 TÉCNICAS DE ATAQUE

Existem diferentes ferramentas que visam facilitar uma invasão em um sistema e diariamente surge uma infinidade de novidades a esse respeito. A seguir serão apresentadas as ferramentas e técnicas de invasão mais conhecidas:

Sniffers: São programas de ataque para o furto de informações dentro de uma rede onde é feita a captura de pacotes. Essa ferramenta analisa o trafego de rede e identifica áreas vulneráveis. Eles representam um alto nível de risco, porque podem ser capturadas senhas de

cartão de créditos e de e-mails. Suponha que sua rede esteja enfrentando lentidões e quedas, isso pode ser um sinal de invasão com sniffers. Exemplos de sniffers: TCPDump e TCPshow; DSniff; mailsnarf; tcpkill; tcpnice.

Engenharia Social: Segundo Allen (2001) o objetivo da engenharia social não é diferente das outras técnicas de crackers: ganho financeiro, interesse pessoal como vingança, pressões externas, vontade e aventura, curiosidade ou destruição de dados. Pode se dizer a engenharia social é um tipo de ataque hacker, onde o instrumento utilizado é a habilidade de lidar com as pessoas persuadindo-as a fornecerem as informações. Estes ataques podem ser feito por salas de bate-papo, telefone, e-mails falsos (spam) ou até mesmo pessoalmente. Fontes (2001) define o termo Engenharia Social como relativamente novo, é aquela conversa que encanta quem está ouvindo e faz com quem o ouvinte fique com total confiança naquele que está falando. O sucesso do ataque depende única e exclusivamente da decisão do usuário em fornecer os dados ou executar certos programas.

Vírus: Segundo a empresa fabricante de softwares antivírus McAfee o primeiro vírus de computador conhecido surgiu no ano de 1986 e era chamado Brain. Era um vírus de boot que atacava o setor de inicialização do disco rígido e se propagava através de um disquete de boot infectado. Vírus de computador são programas desenvolvidos com fins maldosos. Podemos encontrar afinidades em um vírus de computador com um vírus orgânico. Ambos precisam de um sistema ou um programa hospedeiro, o vírus de computador é capaz de se propagar de forma quase sem suspeitas e tal com a gravidade dos vírus dos seres humanos. Eles podem variar de uma pequena inconveniência a um alto grau de destrutividade na máquina. O vírus de computador se abriga com o objetivo de prejudicar o desempenho dele, de apagar arquivos e se propagar para outros computadores.

Exploits: Programas escritos na linguagem C que descobrem a vulnerabilidade de programas e sistemas conseguindo assim acesso root ou administrador. Eles podem estar camuflados dentro de uma mensagem de e-mail ou dentro de determinado comando de um protocolo de rede.

Rootkits: Quando um atacante realiza uma invasão, ele provavelmente vai querer que sua atuação não seja descoberta e que ele possa garantir o seu retorno ao computador afetado. O conjunto de programas que fornecem estes mecanismos é conhecido como rootkit. O termo rootkit não é usado para obter privilégios de administrador do sistema (como é o caso de um exploit), mas para manter estes privilégios ocultos em seus acessos futuros.

Injeção e Modificação de Dados (SQL Injection): SQL é a linguagem usada por bancos de dados para realizar consultas e alterar dados. Um ataque de SQL Injection permite que o hacker

altere de maneira maliciosa os comandos que são passados ao banco de dados. Assim, é possível ler ou alterar dados que normalmente não poderiam ser lidos e alterados. Em vários casos, é possível ler ou alterar as senhas que estão armazenadas no banco de dados, o que procede em uma invasão completa ao site. (Altieres, 2010).

Man in the Middle (MITM): Dá-se o nome de "man in the middle" (homem no meio) a um ataque em que o hacker fica entre a conexão do usuário com o site legítimo que ele quer acessar. Com isso, ele consegue alterar ou ler as informações que o usuário envia. Ataques de "homem no meio" são usados para inutilizar dicas de proteção como àquela que sugere digitar uma senha errada em sites falsos de banco. Se o site falso ficar entre o site legítimo e o usuário, uma senha errada vai retornar erro como no site legítimo. (Altieres, 2010).

Ataques de Força Bruta: Essa é a maneira mais famosa que existe para se quebrar senhas. Consiste em tentar todas as combinações possíveis até que o password seja encontrado. Porém, com o crescimento do tamanho das senhas, as combinações possíveis aumentam exponencialmente e, com isso, também aumenta o tempo necessário para serem decifradas.

Keyloggers: É um software cuja finalidade é monitorar tudo o que é digitado. Muitas vezes esses programas são utilizados com objetivos ilícitos, através de spywares e cavalos de Ttróia. Algumas fraudes virtuais se baseiam no uso de algum tipo de Keylogger, que é instalado no computador sem o conhecimento da vítima, que captura os dados e os envia a um cracker, que posteriormente irá utilizá-los com finalidades dolosas. O Keylogger na maioria das vezes se infiltra no computador da vítima através de e-mails e links falsos. Geralmente, a pessoa só nota que o Keylogger foi instalado depois que o cracker responsável pelo mesmo já tenha entrado no sistema através das senhas capturadas.

Flood: O Flood é uma técnica utilizada para gerar lentidão ou até mesmo derrubar um serviço, ainda mais se o servidor alvo for de pequeno porte. Essa técnica consiste em enviar, sem interrupções, diversos disparos de pacotes para o servidor com objetivo de causar um "congestionamento".

4 MECANISMOS DE SEGURANÇA

4.1 CRIPTOGRAFIA

Segundo Pereira (2007) a criptografia é o ato da transformação da informação em uma forma aparentemente ilegível, com a finalidade de garantir a privacidade, ocultando informação de pessoas não autorizadas. Pelo fato da rede nunca ser completamente segura, devem-se buscar maneiras de torná-la no mínimo mais confiável. Para alcançarmos uma condição de sigilo da informação, podemos contar com os instrumentos e ferramentas da criptografia, para codificar a mensagem de tal forma que apenas um usuário autorizado possa ler de maneira clara e legível.

No seu sentido mais amplo, a criptografia envolve a utilização de mensagens com códigos secretos e cifras. As mensagens escondidas e criptografadas têm como o objetivo não levantar qualquer suspeita. Os códigos em que as palavras e frases são representadas por palavras, números ou símbolos pré-definidos, geralmente são impossíveis de ler, se você não tem o livro com o código da chave criptográfica. Importante para a Segurança da Informação ela serve a várias tecnologias e protocolos, tratando-se de um conjunto de regras e metodologias que visam codificar uma informação de forma que apenas o emissor e o receptor possam acessá-la e entende-la, evitando que um intruso consiga acessar a mensagem.

A Criptografia tem suas origens há muitos anos. Comenta-se que o imperador romano Júlio César teria sido o primeiro a empregá-la, porque não confiava no mensageiro e havia o risco dele ser capturado, no caso de uma guerra. O método utilizado por César era simples: ele reescrevia a carta somando 3 a posição da letra, ou seja, o "A" (1) passaria a ser "D" (4), o "B" (2) "E" (5) e assim sucessivamente, imaginado as letras dispostas em círculo, ou seja, a lista não termina no "Z" mas continua daí no "A" novamente.

Cada letra ou grupo de letras na mensagem é substituído por outro na mensagem cifrada. Esta substituição é realizada para tornar o texto cifrado mais incompreensível. A decifragem é feita realizando-se a substituição inversa, de forma a restaurar os caracteres do texto original (TANEMBAUM, 2003).

Para que a criptografia seja realizada, o ciframento (embaralhar a mensagem, criptografar) e o desciframento (operação inversa, desembaralhar a mensagem, descriptografar) se utilizam de um algoritmo nomeado "chave criptográfica", de maneira que a decifração, em princípio, somente é possível conhecendo-se a chave apropriada para decifrar, mesmo que se conheça o algoritmo utilizado.

4.1.2 Algoritmos Criptográficos

Terada (2000) descreve que os algoritmos criptográficos basicamente objetivam "esconder" informações sigilosas de qualquer pessoa desautorizada a lê-las, isto é, de qualquer pessoa que não conheça a chamada chave secreta de criptografia. O uso de criptografia cresce de acordo com a internet, os sites das companhias precisam que usuários se identifiquem ao acessar às suas páginas privadas. Quando o usuário digita a senha para obter o acesso, algoritmos de criptografia são executados para reconhecer a senha digitada. Caso a sequência criptográfica gerada através da senha do usuário for à mesma que o sistema tem em seu banco de dados, o usuário é autenticado, podendo assim ter acesso ao site.

Existem duas categorias de algoritmos criptográficos: simétricos (chave-secreta) e assimétricos (chave-pública). Os algoritmos simétricos utilizam uma mesma chave tanto para cifrar como para decifrar, ou seja, a mesma chave utilizada para fechar a mensagem é utilizada para abrir a mensagem, quando uma pessoa vai se comunicar com outra, ela gera a chave e a transmite por um canal seguro para a segunda pessoa. Assim a mensagem é criptografada com essa chave e a outra pessoa descriptografa com a mesma chave.

Figura 1 - Exemplo de algoritmo simétrico
Fonte: Cardia (2009)

Exemplos de algoritmos de chave simétrica:

DES - Data Encryption Stardard, O DES processa blocos de texto de 64 bits cada vez, usando uma chave de 56bits, produzindo um texto cifrado de 64bits. O DES para causar um efeito mais interessante faz este procedimento 16 vezes, cada uma usando uma porção diferente da chave.

O AES – Padrão Avançado de Ciframento (Advanced Encryption Standart) é um algoritmo simétrico que pode usar chaves de 128, 192 ou 256 bits com blocos de dados de 128 bits.

Nos algoritmos assimétricos são usadas chaves distintas, uma para cifrar e outra para decifrar e, além disso, a chave de decifração não pode ser obtida a partir do conhecimento da chave de cifração apenas. Aqui, uma chave é utilizada para "fechar" e outra chave, diferente, mas relacionada à primeira, tem que ser utilizada para "abrir".

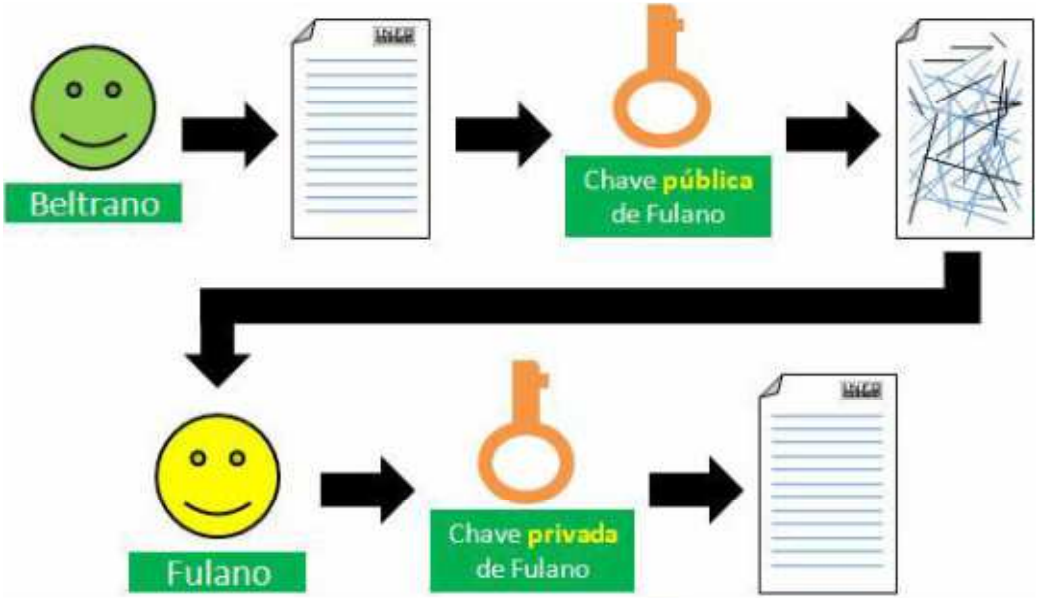

Figura 2 - Exemplo de algoritmos assimétricos
Fonte: Alecrim (2009)

Exemplos de algoritmos de chave assimétrica:

RSA - É um dos principais algoritmos de segurança utilizado na Internet para transações comerciais. Ele é baseado na construção de chaves públicas e privadas utilizando números primos.

ECC - (Eliptic Curve Cryptography ou algoritmo de Criptografia de Curvas Elípticas). Neste método utiliza-se uma chave de 160 bits enquanto que outros algoritmos como o RSA utiliza uma chave de 1024 bits. O algoritmo de Criptografia de Curvas Elípticas é considerado seguro e veloz em suas execuções.

4.2 ASSINATURA DIGITAL

É necessário se pensar em algo como uma assinatura digital para que o registro de algum fato ocorrido na web possa ser igualado a um documento formal, pois a segurança é atualmente a maior preocupação de todos que negociam pelos meios eletrônicos. A credibilidade dos documentos está ligada a sua originalidade e a certeza de que ele não foi alterado até chegar ao seu destinatário.

A assinatura digital tem seguintes propriedades:

- Um usuário não pode falsificar a assinatura de outro usuário;
- As assinaturas digitais devem ser únicas para cada usuário;
- O emissor da mensagem não pode anular a assinatura de uma mensagem, ele não pode negar o envio de uma mensagem com sua assinatura;
- Um usuário não pode ser capaz de retirar a assinatura de uma mensagem e colocar em outra;

Exemplo de como funciona a assinatura digital:

Ana precisa mandar uma mensagem assinada para Carlinhos, ela tem uma chave privada de assinatura e uma chave publica de verificação. Qualquer um (incluindo Carlinhos) pode utilizar a chave publica de Ana para verificar a assinatura ao receber mensagens enviadas por ela. Apenas Ana pode assinar corretamente (com sua chave privada) as mensagens.

4.3 FIREWALL

A palavra Firewall traduzida para o português significa "muralha de fogo", fazendo referência a uma área restrita, resguardando a segurança interna nas empresas em um ambiente de rede.

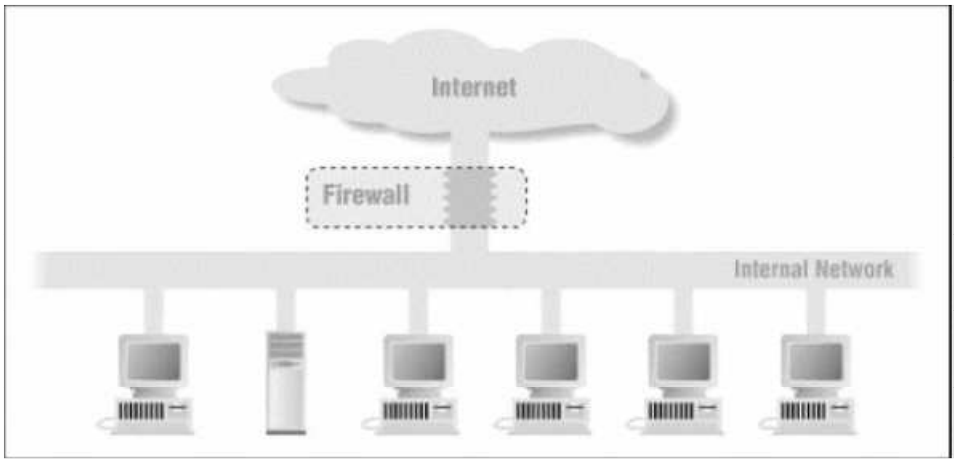

Figura 3 - Posicionamento do Firewall na Rede de Computadores
Fonte: ZWICKY (2000)

Um firewall é um sistema que impõe uma política de controle de acesso entre duas redes, tendo as seguintes propriedades:

- Todo tráfego de dentro para fora de uma rede, e vice-versa, deve passar pelo firewall.
- Apenas tráfego autorizado, como definido pela política de segurança local, terá permissão de passar.
- O próprio firewall deve ser imune a penetrações.

Apenas a instalação de um firewall não garante que uma rede esteja segura contra invasores e ataques. Sendo assim, um firewall não pode ser a única linha de defesa, ele é mais um dentre os diversos mecanismos e procedimentos que aumentam a segurança de um sistema. Outro limite dos firewalls é que eles protegem apenas contra ataques externos ao firewall, nada podendo fazer contra ataques que partem de dentro do sistema por ele protegida.

Pereira (2007) lista algumas das limitações do firewall:

- Ataques internos e usuários mal intencionados;
- Proteção antivírus;
- Portas abertas (Backdoors);
- Falhas no equipamento

Para entender a tecnologia empregada nas implementações de firewalls, é necessário conhecimentos em objetos com os quais o firewall lida: pacotes e protocolos. Para transferir informações por uma rede, elas devem ser quebradas em pequenas partes, transferidas uma a

uma separadamente. Quebrar as informações em pedaços permite a muitos sistemas dividirem a rede, cada um mandando partes de sua informação, na sua vez.

Um firewall pode se comportar como um roteador, filtrando pacotes oriundos da internet baseados na informação contida em cada datagrama pelo meio da análise de informações como endereço de origem, endereço de destino e protocolo usado para a comunicação. Em algumas situações ele pode se comportar como um proxy servers impedindo o acesso direto à Internet. Ele filtra acessos não autorizados aplicando restrições de tráfego. Firewalls agem como um portal de segurança (TREVENZOLI, 2006).

4.4 ANTIVIRUS

Como o próprio nome diz, os antivírus são ferramentas utilizadas para proteger os computadores contra diversos tipos de vírus. Os antivírus podem ser divididos em duas categorias: gratuitos e por assinatura. Para melhorar a efetividade do antivírus, são necessárias constantes atualizações, conforme esclarecem Silva, Carvalho e Torres (2003):

> Estas soluções obrigam a permanente atualização das bases de dados de assinaturas (e, com menos frequência, dos motores de detecção e de remoção), bem como a disseminação dessas atualizações por todos os sistemas a proteger. A consequência, caso não exista um cuidadoso planejamento prévio, pode ser um enorme esforço de atualização dos produtos antivírus existentes que, ao ritmo de aparecimento de novos vírus, pode tornar-se uma batalha perdida.

Lista de alguns programas de anti-virus disponiveis no mercado:

- Norton Antivírus, da empresa Symantec
- F-Secure Anti-Virus, da empresa F-Secure
- Panda AntiVírus, da Panda Software
- Avira AntiVir Personal - Free Antivirus, da empresa Avira
- Avast!, da empresa Alwil
- AVG Anti-vírus, da empresa AVG Technologies

4.5 BACKUP

Sobre os vários tipos de ameaças existentes ainda há aquelas que podem atacar os sistemas de informação provocando a eliminação de determinados arquivos que fazem com

que os sistemas não funcionem corretamente, é por essa razão que existem os backups, que são meios de fazer uma cópia em local separado e seguro. Devido à importância da informação para uma empresa, é essencial que se realize o backup diariamente para evitar falhas no sistema e problemas de hardware.

Com os serviços atuais de grandes empresas de tecnologia é possível ter uma cópia dos seus backups e arquivos que quiser nas nuvens, onde você pode acessar de onde estiver. Os serviços de armazenamento online acabam com o problema de quem não dispõe de espaço físico para servidores. O serviço de backup nas nuvens é de natureza prática, pois dispensam qualquer tipo de mídia física para armazenamento. A escolha de um serviço confiável para prestação de backup é essencial. A dica para o usuário, seja pessoa física ou jurídica, é testar as ferramentas disponíveis. A maioria das empresas que presta serviços de backup nas nuvens oferecem pacotes gratuitos com espaço de armazenamento limitado ou períodos de teste (Flávio Santos de Araújo, 2012).

4.6 SENHAS

Para impedir o acesso de outra pessoa com a sua identificação no sistema deve-se atentar em alguns aspectos relativos à construção da mesma. É aconselhável que na elaboração de senhas os seguintes conselhos sejam seguidos:

- Elaborar senhas que contenham no mínimo oito caracteres, compostos por números, letras e símbolos.

- Nunca utilizar como senha seu nome, sobrenomes, números de documentos, placas de carros, telefones ou datas que possam ser relacionadas com você ou encontradas em dicionários.

- Utilizar uma senha diferente para cada serviço. Evita que o atacante ao descobrir uma senha obtenha acesso a todos os seus serviços.

- Alterar a senha com certa frequência

4.7 MEDIDAS DE SEGURANÇA EM RECURSOS HUMANOS

A medida de segurança em recursos humanos está relacionada às pessoas que trabalham e colaboram com a organização. As pessoas são essenciais para a organização. O treinamento dos usuários tem o objetivo de informar aos funcionários novos e antigos as

regras da organização e políticas que devem ser seguidas. Com isto, a organização define um comportamento para as pessoas dentro da empresa minimizando as chances do ataque de engenharia social. A continuidade do negócio é o maior ganho para a empresa que fornece treinamentos para os usuários.

Algumas medidas devem ser seguidas:

- Nunca fornecer dados pessoais como números de cartões e senhas através de contato telefônico.

- Estar atento a e-mails ou telefonemas solicitando dados pessoais.

- Não acessar sites ou links recebidos por e-mail ou presentes em páginas sobre as quais não se tenha certeza da procedência.

- Sempre que houver receio sobre a identidade do autor de uma mensagem ou ligação telefônica, entrar em contato com a instituição em questão para verificar a veracidade dos fatos.

4.8 FERRAMENTAS PARA DETECÇÃO DE VULNERABILIDADES

Frente ao grande número de vulnerabilidades reportadas diariamente em listas de discussão e sites relacionados à segurança, torna-se difícil para gerenciadores de redes e consultores de segurança efetuar todos os testes necessários para assegurar a integridade de seus sistemas. Para tentar solucionar esse problema, surgem os softwares de detecção de vulnerabilidades. Estes programas não cobrem todas as vulnerabilidades possíveis, porém torna esse processo mais rápido e eficaz. É extremamente importante realizar um diagnóstico de segurança do ambiente para a definição da melhor estratégia de proteção para qualquer empresa. Além do conhecimento sobre a natureza de ataques e sobre diferentes aspectos envolvidos com a segurança (tecnologias, processos, pessoas), o diagnóstico também envolve o conhecimento sobre as técnicas e as ferramentas utilizadas.

4.8.1 Ferramentas de Pesquisa a Vulnerabilidades

Existem várias ferramentas de análise de vulnerabilidades sejam elas comerciais, open source ou de utilização livre. Ferramentas distintas conseguem encontrar diferentes vulnerabilidades, isto devido à técnica de análise utilizada e também aos tipos de vulnerabilidades para os quais as ferramentas foram desenvolvidas. Abaixo são listados

alguns dos diversos softwares disponíveis e uma breve descrição de seu funcionamento com link para download.

Nmap - Network Mapper é uma ferramenta livre e de código aberto para exploração de rede e auditoria de segurança. O Nmap utiliza pacotes IP em estado bruto para determinar quais os hosts que estão disponíveis na rede, quais os serviços que os hosts oferecem e qual o sistema operacionail e sua versão que estão a executar e que tipos de firewall. O Nmap, de uma forma geral, fornece a relação de computadores e serviços ativos por métodos e argumentos muito simples. Ele pode ser executado no Linux/Unix ou em Windows.

Link para download: http://www.nmap.org

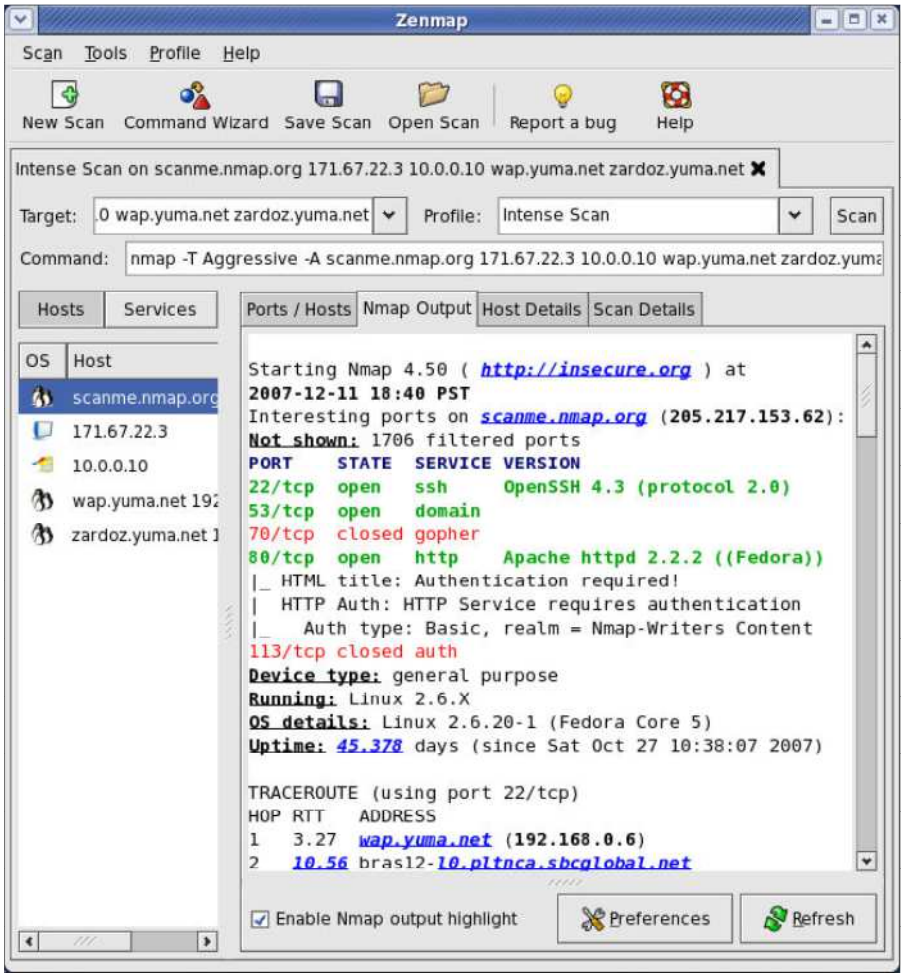

Figura 4 - Ferramenta nmap
Fonte: http://www.nmap.org

GFI LanGuard - É uma ferramenta única no fornecimento de gerenciamento de pacotes, avaliação de vulnerabilidades e auditoria de redes. Com essas três funções inclusas,

ele reduz o custo total das suas ferramentas essenciais de segurança. Ele também lhe auxilia no inventário de ativos, gerenciamento de mudanças, analise de riscos e comprovação de conformidade.

Link para download: http://www.gfi.com/downloads/register.aspx?pid=lanss.

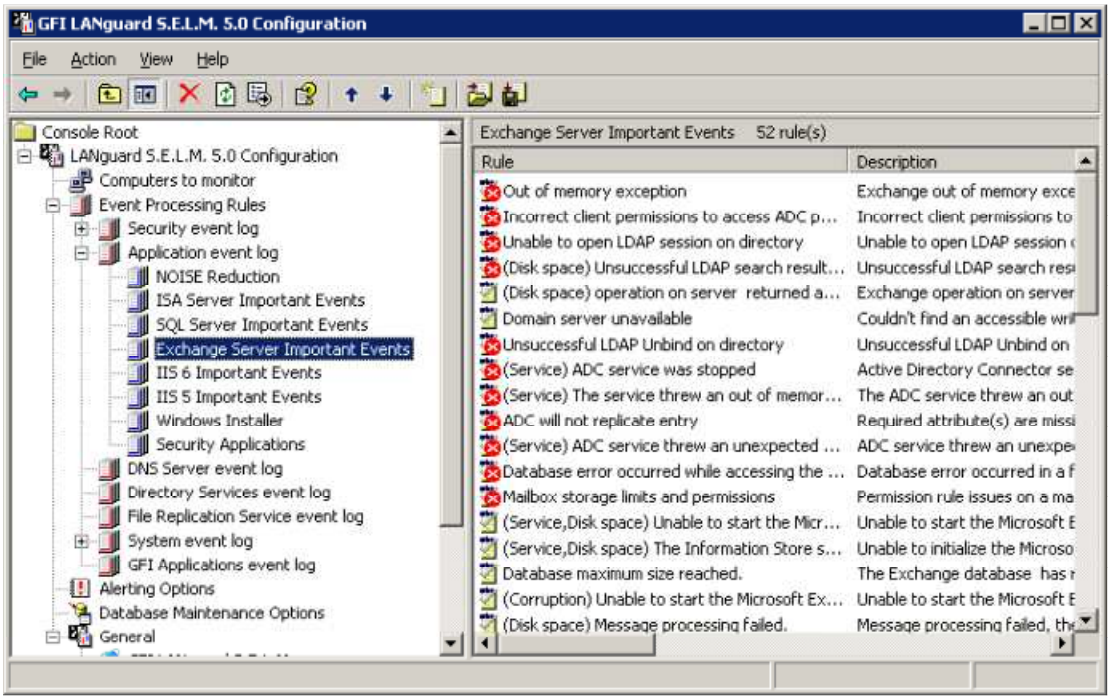

Figura 5 – Ferramenta LanGuard
Fonte: http://www.gfi.com

Nessus - é um freeware, possui interface própria simples e fácil de operar que trabalha com o conceito de cliente e servidor. O servidor é quem de fato efetua os testes e o módulo cliente envia requisições de testes e avalia seus resultados. Assim sendo esses dois módulos podem estar em hosts diferentes ou também serem executados no mesmo host. A fim de evitar clientes "falsos", o servidor tem o recurso de cadastro de usuários para conexão a partir dos clientes e endereços IPs de hosts ou redes permitidos para aceitar conexões. Para a comunicação entre cliente e servidor é utilizada autenticação de usuários e métodos de criptografia. Link para download: http://www.tenable.com/products/nessus.

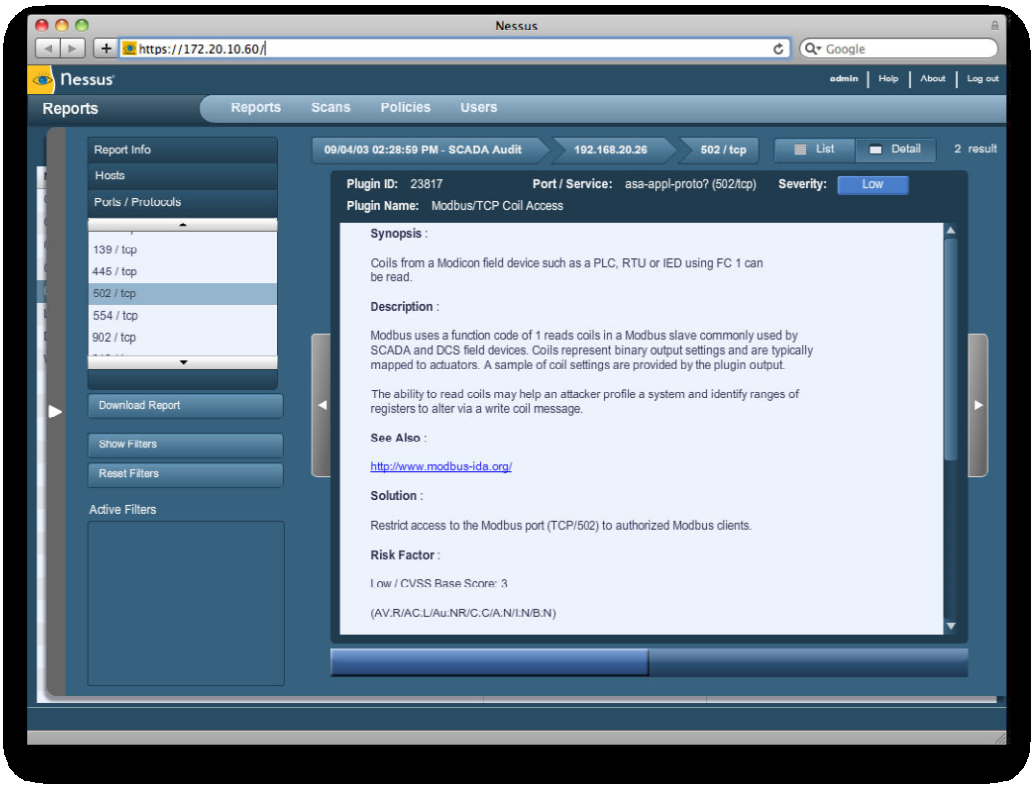

Figura 6 – Ferramenta Nessus
Fonte: http://www.tenable.com

5 POLITICAS DE SEGURANÇA

Política de segurança é uma declaração formal das regras que devem ser obedecidas pelas pessoas que tem acesso à tecnologia e às informações da empresa. Uma política de segurança é fundamentalmente um documento que resume como a corporação utilizará e protegerá seus recursos computacionais e de rede (SILVA, 2006).

As decisões relacionadas à segurança que devem ser tomadas em grande parte determinam o quão segura ou insegura sua rede é. Quanta funcionalidade a rede oferece e o quão fácil ela é de ser utilizada. Porém, não se pode tomar boas decisões sem determinar primeiro quais são as metas de segurança para a empresa. A segurança de um sistema não se resume apenas à utilização de dispositivos físicos que tentam impedir que este fosse atacado ou invadido, mas também de que forma os dispositivos serão aplicados e quem terá acesso aos recursos e como eles devem ser acessados.

A política de Segurança da Informação é um mecanismo preventivo que propende à proteção dos dados de uma empresa. Ela define um padrão de regras de segurança a serem seguidas por todos os usuários dos sistemas da informação. Uma política de segurança é a formalização de todos os aspectos considerados relevantes por uma organização para a proteção, domínio e monitoramento de seus recursos computacionais e consequentemente das informações por eles manuseadas (SANTOS, 2005).

A política de segurança deve contemplar, de forma genérica, todos os aspectos importantes para a proteção lógica e física das informações e dos recursos computacionais.Para Ribeiro (1998), o objetivo da política de segurança abrevia-se em manter sob controle o armazenamento da informação, que na maioria das vezes, é o mais bem mais valioso de uma empresa devendo seguir estes quatro paradigmas básicos:

- Integridade: A condição na qual a informação ou recursos da informação é protegido contra modificações não autorizadas.

- Confidencialidade: Propriedade de certas informações que não podem disponibilizadas ou divulgadas sem autorização prévia do seu dono.

- Disponibilidade: Característica da informação que se relaciona diretamente à possibilidade de acesso por parte daqueles que a necessitam para o desempenho de suas qualidades.

- Legalidade: Estado legal da informação, em conformidade com os preceitos da legislação em vigor, no que se refere à aplicação de medidas punitivas.

Segundo a norma ISO/IEC 17799, o objetivo é de uma política de segurança é prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

As políticas de segurança são elaboradas de um conjunto de regras e padrões sobre o que deve ser feito para cobrir as informações e serviços importantes.

Segundo Marinho (2007), um plano de segurança deve conter:

- Uma lista dos serviços de rede que serão oferecidos;
- Quais áreas da organização proverão os serviços;
- Quem terá acesso a esses serviços;
- Como será provido o acesso;
- Quem administrará esses serviços;

5.1 ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

Para Azeredo (2007), a estrutura normativa da Segurança da Informação é composta por um conjunto de documentos com três níveis hierárquicos, listados a seguir:

Política de Segurança da Informação: Define a estrutura, as diretrizes e as obrigações referentes à segurança da informação. Possui um papel estratégico, pois precisam expressar a importância que a informação possui para a empresa, além de comunicar aos empregados seus valores e seu comprometimento em desenvolver a segurança para a organização da empresa.

Normas de Segurança da Informação: Estabelecem procedimentos definidos de acordo com as diretrizes da política, a serem seguidos em diversas situações em que a informação é tratada. As normas para uma política de segurança da informação deverão conter critérios normatizados para admissão e demissão de funcionários; criação de senhas; descarte de informação em mídia magnética (CDs, HDs); uso da Internet; uso de notebooks; contratação de serviços terceirizados;

Procedimentos de Segurança da Informação: Instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades da empresa. Os procedimentos possuem um caráter mais operacional, corresponde a maior parte da política de segurança da

informação devido ao fato de terem que apresentar e descrever meticulosamente cada ação e atividade associada a cada situação apontada do uso das informações.

De acordo com a norma NBR ISO/IEC 17799:2005 uma política de Segurança da Informação tende prover uma orientação e apoio da direção para a segurança de acordo com os requisitos do negócio e com as leis e regulamentações relevantes, com o alvo de minimizar as preocupações dos membros da direção da empresa com a segurança de seus recursos e informações.

A política de segurança pode trazer ao ambiente de uma instituição, regras e procedimentos que devem ser seguidos para a garantia da segurança da informação. É importante que as informações da política de segurança sejam divulgadas para todos os membros da instituição, funcionários, colaboradores ou estagiários, e que todos estejam conscientes da importância do seguimento desta política (SPANCESKI, 2005).

Aliado as políticas de segurança deve existir o Termo de Compromisso, com a identificação do empregado declarando que o mesmo está ciente das políticas de segurança, tem conhecimento de suas responsabilidades e concorda em desempenhar o que está determinado.

Logo abaixo serão citados os elementos que precisam estar inclusos na prática de uma boa politica de segurança:

- Segurança física: É aquela que envolve aspectos como prevenção contra falhas de equipamentos incêndios, acesso de pessoas a locais restritos, enchentes, desastres naturais, acidentes, roubo e demais aspectos físicos (SOUSA, 2005) No domínio da informática, a segurança física dos sistemas refere-se à proteção de equipamentos e instalações contra riscos por extravios ou por danos físicos. Inclui componentes como controlos de acesso, serviços contra incêndios e dispositivos para a detecção de infiltrações de água.

- Segurança do pessoal: Segundo Silva (2005) a segurança do pessoal é um aspecto muito importante dado que são as pessoas que interagem diariamente com os sistemas, que tem acesso às informações contidas no sistema, por isso muitas vezes são as principais ameaças a esses sistemas. Carvalho (2002) defende que se deve ter muito cuidado no recrutamento de pessoas, porque estas podem ser possíveis perigos à segurança nas organizações.

- Resposta a incidentes: Um incidente de segurança é qualquer caso que pode causar perda e dano dos recursos da organização, uma ação que afete os procedimentos de segurança na organização. Carvalho (2002) defende que o conhecimento desses incidentes por parte dos utilizadores do sistema é fundamental para minimizar as consequências que advém destes

incidentes, por isso, é muito importante que estes saibam a forma mais fácil e rápida para comunicar estes incidentes. Neste caso a formação de utilizadores neste aspecto é fundamental para solucionar problemas, quando acontecer qualquer incidente.

- Segurança lógica: Abrange aspectos de prevenção contra interceptação de informações, sigilo no tráfego dos dados na rede, alterações de softwares, invasões em sistema. A segurança lógica associa-se á proteção dos dados e dos programas, a segurança da utilização dos programas ao acesso autorizado dos utilizadores.

5.2 A IMPLEMENTAÇÃO DE UMA POLITICA DE SEGURANÇA

Normalmente a implementação de uma política de segurança é considerada a parte mais complexa. Sua criação envolve muitas variáveis, como: ambiente de rede, organização, tecnologia e pessoas. Contudo, a execução da implementação é avaliada como a maior dificuldade desse processo de política de segurança, pois leva um pouco de tempo para que as pessoas entendam e cumpram as designações. Isso faz com que um ponto importante para a aceitação e conformidade com a política definida seja a educação (NAKAMURA, 2007). Os empregados devem ter a consciência do valor que tem a política de segurança, para que não a torne inoperante de modo a reduzir sua eficiência. A completa implantação da segurança da informação pode levar até anos para conseguir os resultados cobiçados, logo é importantíssimo que esse planejamento seja bem realizado.

6 ANÁLISE PRÁTICA

A característica exploratória da análise prática é extremamente importante para verificar situações de Segurança da Informação em organizações. A estratégia de pesquisa baseada em análise prática diz respeito à investigação de um fenômeno dentro de um ambiente específico. Assim, essa técnica diz respeito à pesquisa de um objeto com vistas a compreendê-lo de forma ampla em seu contexto.

Segundo Fernandes (2010), pesquisas baseadas em análise prática podem tanto descrever uma determinada configuração de ambiente, como também servir de pressuposto a generalizações.

6.1 CARACTERIZAÇÃO GERAL

Com a finalidade de auxiliar na compreensão de alguns passos na avaliação de riscos e questões relevantes para a Segurança da Informação em redes corporativas, utilizou-se como exemplo uma empresa que atua no ramo de provedores de internet, a SOLNET, localizada na Rua Vidal de Negreiros, 94 Patos - PB.

O desempenho das etapas da avaliação de riscos tem como objetivo identificar falhas relacionadas à Segurança da Informação em estruturas tecnológicas para a minimização dos riscos após estudos das ocorrências e impactos. Almeja-se compreender aspectos da estimativa de riscos para assimilação das precisões de segurança da empresa e avaliar a praticidade de metodologias de avaliação como a elaboração de uma boa política de Segurança da Informação.

6.2 ESTRUTURA ORGANIZACIONAL

A empresa foi definida por um dos gerentes sócios como uma empresa de médio porte que utiliza um sistema para atender grandes clientes. A SOLNET procura ser referência no ambiente de provedores de internet fornecendo o acesso à internet de maneira prática e fácil para empresas e usuários domésticos.

É administrada por dois sócios e têm em seu quadro funcional:

- Sete funcionários atendentes/secretários;
- Dezessete funcionários na área de suporte;
- Três empregados na área comercial;

- Dois gerentes administrativos;

As operações de negócio se iniciam através do contato inicial com o cliente. Após esclarecimentos se houver comum acordo, o cliente assina um contrato de uso e aluguel de programas e serviços. A SOLNET fica responsável por instalar os equipamentos e documentar todos os parâmetros dos clientes a serem utilizados no sistema. Daí por diante a empresa segue suas atividades oferecendo seus serviços de suporte e auxílio.

6.3 DESENVOLVIMENTO

O começo da estimativa de riscos está catalogado ao levantamento de informações da empresa para identificar a afinidade entre cada operação de computação que dão apoio às tarefas de cada funcionário da empresa. O objetivo é identificar ameaças potenciais dos riscos ao negócio que oriente os valores de segurança corporativa. Através de uma entrevista com o sócio da empresa procurou-se identificar os processos críticos considerando que os atos de segurança necessitam ser priorizadas para o normal andamento dos negócios. Os contatos iniciais foram feitos por telefone e e-mail. As entrevistas foram realizadas pessoalmente, junto à empresa objetivando respostas sérias e corretas. A pesquisa foi aplicada na forma de entrevistas pessoais com os responsáveis pela área de segurança da empresa. O questionário usado foi baseado no artigo Importância da Segurança da Informação: Um estudo de caso em uma Empresa de Telecomunicações do autor Francisco Eudes Pinto de Andrade que se encontra disponível nos anexos. Pelo meio das informações colhidas, foi possível estudar o perfil da empresa e funcionários, o grau de consciência e responsabilidade dos envolvidos e a segurança propriamente dita, falhas, tecnologias e ameaças.

Nos primeiros encontros, foram esclarecidos quais serviços são prestados e como as operações de negócio ocorrem com auxílio das respostas do gerente/sócio. Após breve discussão sobre a metodologia de avaliação e possíveis benefícios, foi dado início ao preenchimento do questionário do processo que objetiva estabelecer critérios de avaliação de impactos. Foi notado que estes critérios podem ser muito subjetivos e muitas vezes complexos de serem medidos para avaliar o impacto de riscos à Segurança da Informação, mesmo através da discussão sobre esse tópico com membros que tenham um bom entendimento das operações da organização.

Foi definido que:

- A credibilidade com o cliente, quando comprometida representa um risco de elevado impacto para a empresa. As consequências são evidentes caso algum funcionário da empresa opere indevidamente na base de dados do cliente para manutenção.

- Para cada serviço é estipulado um prazo, caso ocorra alguma interferência à produtividade diminui e conseqüentemente os rendimentos caem. Qualquer risco que afete a produtividade da empresa foi considerado como de alto impacto por atrasar a conclusão do serviço trabalhado.

Considerações como estas são importantes para analisar impactos nos negócios causados por ameaças específicas e apresentar as diretrizes e normas da política de segurança corporativa que aloque padrões de segurança para o uso de serviços e equipamentos da rede. Os requisitos de confidencialidade, integridade e disponibilidade do serviço foram considerados importantes, pois somente pessoal autorizado pode visualizar a informação sobre os clientes da empresa ou modificar registros. Foi tratada também a avaliação quanto às práticas de segurança atuais para o gerenciamento de segurança, observação de políticas de segurança e regulamentos. Tudo isso se mostrou muito útil como reflexão das práticas adotadas para guardar o patrimônio da empresa que adota as seguintes medidas de segurança:

- Gerenciamento de e-mails para manter o sigilo das informações
- Filtragem de conteúdo das páginas acessadas na Internet para evitar o acesso às páginas impróprias

6.3.1 Instrumentos de Coleta de Dados

O questionário sobre Segurança da Informação que está disponível no anexo A contém vinte e cinco questões distribuídas em dois tópicos, que são descritos a seguir:

a) Perfil da organização entrevistada:

   É uma empresa de pequeno a médio porte, localizada na cidade de Patos-PB que oferece serviço de provedor de internet para empresas e usuários domésticos.

b) Consciência dos funcionários e responsáveis pela área:

   Conscientização é muito importante, saber como a política de Segurança da Informação é vista pelos funcionários da área reflete a verdadeira situação da segurança da informação da organização. Este tópico trata também sobre o orçamento destinado ao setor de segurança e como acontece a aplicação destes recursos.

c) Informações sobre as falhas na segurança:

Este tópico trata de vulnerabilidades e que tipo de procedimento é adotado pelos responsáveis nas áreas de segurança. Trata do uso corporativo da internet e as soluções adotadas para proteção de documentos na internet.

Foram feitas questões de múltiplas escolhas a fim de facilitar as respostas e a tabulação das mesmas. Dessa forma, foi possível coletar informações a respeito de vulnerabilidades nas políticas de segurança da empresa.

6.4 RESULTADOS

A partir da pesquisa realizada observou-se que as práticas de segurança tomadas servem para o controle mínimo necessário, com o fim de dar continuidade às operações básicas. É muito comum encontrar no ambiente de muitas empresas um firewall implementado, ferramentas para filtragem de conteúdo das páginas internet, gerenciamento de e-mail, prevenir a instalação de vírus, controlar o tráfego da rede, porque estas soluções de segurança estão ficando mais acessíveis e são muito importantes. Contudo, não há uma preocupação em elaborar uma documentação orientadora de normas, regras e instruções de Segurança da Informação para a companhia ou mesmo esforço para se adaptar às recomendações de normas de boas práticas de segurança. Isto pode ocorrer devido aos seus administradores terem um bom controle do ambiente de trabalho e também porque não existem registros de incidentes de segurança graves ocorridos antes. As instruções são passadas verbalmente e os administradores reconheceram não haver um controle severo da segurança.

Não é incomum que o corpo administrador tenha uma visão delimitada sobre segurança apenas pelos fatores tecnológicos e sendo assim, a empresa dá andamento normal das suas atividades sob uma impressão de segurança que pode muitas vezes ser falsa.

Mesmo que as regras de filtragem de um firewall tenham sido bem configuradas, pode se compor um ponto de ataque à rede e atalho de desvio da filtragem de pacotes implementada. Em outro caso, se um sistema operacional não for atualizado com os pacotes de segurança disponíveis pela fabricante, a rede poderá estar vulnerável também a outros tipos de exploração de falhas. Caso um agente motivado (funcionário demitido, hacker) se empenhe em prejudicar a rede empresarial, é possível que não encontre muitas dificuldades.

Uma política de Segurança da Informação pode prever testes de segurança para verificar o estado atual de proteção do patrimônio tecnológico da corporação. Pode-se dizer que mesmo a rede coorporativa sendo de baixo a médio porte, não havendo registros de

incidentes de segurança e existindo um controle suficientemente bom do número de funcionários, uma política de segurança não deixa de ser uma ferramenta de apoio à segurança para orientar a empresa sobre aquisição, configuração e implementação das ferramentas que melhorem o nível de proteção. Sabe-se que os recursos de computação estão sendo sempre otimizados e novas ferramentas são lançadas no mercado rapidamente.

Por meio das reflexões sobre segurança que uma metodologia de avaliação de riscos proporciona, entende-se que um sistema de computação nunca estará cem por cento protegidas. A política de segurança pode também ser necessária caso a companhia tenha projetos de expansão para atuar em outros pontos da cidade ou em municípios diferentes, isso facilitará o repasse dos requisitos de segurança importantes da organização.

Para responder ao questionamento que deu origem a este trabalho, a saber, a importância da segurança da informação para a organização. As seguintes problemáticas foram avaliadas:

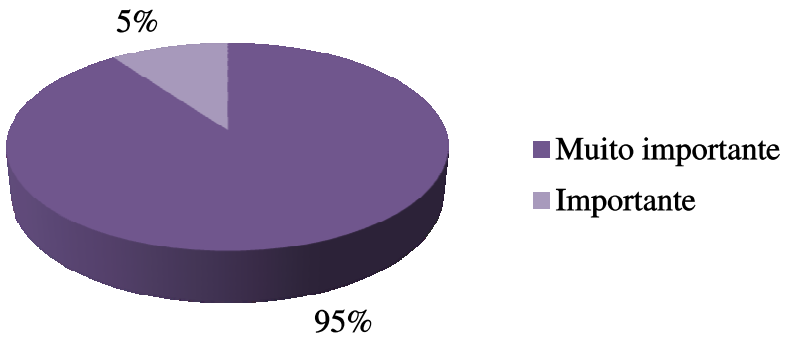

Gráfico 1 - Importância da segurança da informação

Fonte: Pesquisa direta

Em entrevista 95% dos funcionários acham que a Segurança da Informação é muito importante na empresa. Os outros 5% consideram importante.

Continuando com a pesquisa, foram questionados quais os principais obstáculos para que uma boa política de Segurança da Informação seja implementada de forma eficiente.

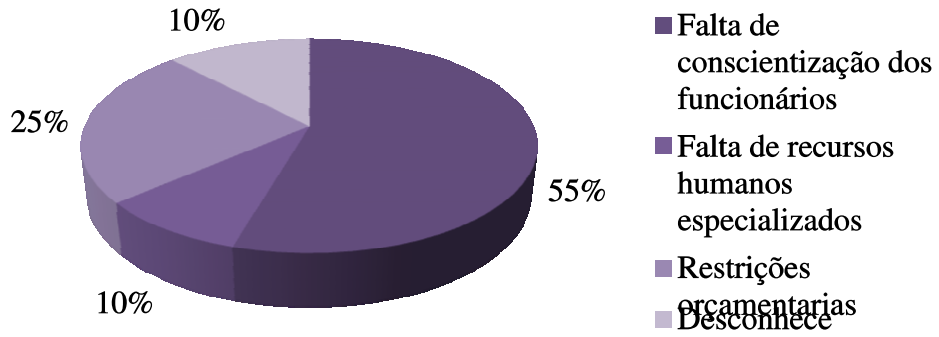

Gráfico 2 - Obstáculos para implementar política de segurança

Fonte: Pesquisa direta

Observa-se que a maioria dos que responderam (55%) considera que a maior barreira é a falta de conscientização dos próprios funcionários e ausência de recursos humanos especializados (10%). Outro motivo citado são as restrições orçamentárias (25%) alguns administradores usam deste quesito como justificativa para o não investimento em politicas de segurança corporativa ou até mesmo por considerar como despesa o investimento realizado na segurança e (10%) responderam desconhecer os obstáculos que impedem esta política.

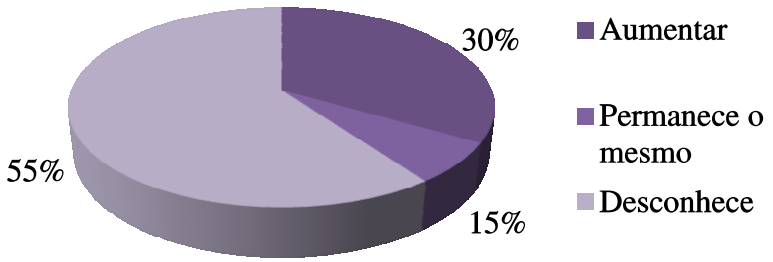

Gráfico 3 – Investimentos para a empresa em segurança da informação em 2013

Fonte: Pesquisa direta

O gráfico 3 confirma que há uma grande quantidade de funcionários (55%) que desconhecem sobre investimentos na área de Segurança da Informação, mas se percebe que uma mostra de entrevistados (30%) afirma que tais investimentos irão crescer no ano de 2013, e apenas (15%) consideram que irá continuar o mesmo para o próximo ano.

Gráfico 4 - Maiores perigos para a informação da empresa

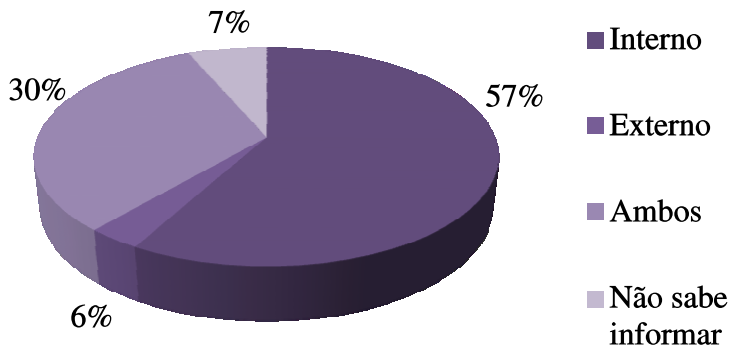

Gráfico 5 - Maiores perigos para a informação da empresa

Fonte: Pesquisa direta

Foram destacados pelos entrevistados (57%) que o maior perigo para os ativos da organização são os internos. Isto apresenta, como no início da pesquisa, a insatisfação dos funcionários, prestadores de serviço e usuários, que são a maior fonte de atenção do departamento de segurança da informação. Apenas (6%) dos entrevistados consideram os atacantes externos como ameaça real às informações; enquanto que (30%) consideram ambos, internos e externos, o verdadeiro perigo e outros (6%) não sabem informar.

Através do questionário, a possibilidade de adoção de práticas de segurança que podem servir para o melhor gerenciamento da segurança foi avaliada. Sinais de alerta (vermelho, amarelo, verde) foram dadas para a política de segurança para avaliar quão eficiente têm sido a implementação dessas medidas de segurança.

Receberam o status vermelho e amarelo respectivamente, que podem ser melhoradas a partir da adoção de práticas como:

- Estabelecimento de um plano de teste de segurança da rede, com o uso de ferramentas de detecção de vulnerabilidades para execução pelo menos uma vez por semana.

- Designação de responsabilidade para um dos funcionários verificar regularmente a integridade dos softwares instalados.

- Apesar de que a empresa não tenha registros de ataques, é aconselhado a utilização dos registros de log para auditoria e ferramentas de mapeamento de vulnerabilidades.

- Os equipamentos críticos (recursos do sistema e da rede) não devem estar indisponíveis por mais do que uma hora.

Receberam o status sinal verde:

- Os softwares estavam atualizados e sem indícios de pirataria que poderiam afetar a integridade do sistema.

- Os procedimentos para a verificação de toda informação relacionada a código malicioso e garantia de que os alertas sejam precisos e informativos.

- Verificação, antes do uso, da existência de vírus em qualquer arquivo em meio magnético de origem desconhecida ou não autorizada, e em qualquer arquivo recebido a partir de redes não confiáveis.

- Os planos de contingência estão adequados para a recuperação em caso de ataques por vírus, incluindo os procedimentos necessários para salva e recuperação dos dados e software.

- São efetuadas rondas semanais pelas instalações e serviços da SOLNET, com o intuito de fazer uma manutenção preventiva.

Uma documentação de segurança, mesmo que inicialmente simples e voltado a apenas algumas áreas funcionais da empresa pode ajudá-la com adoção de novas práticas de segurança essenciais para o gerenciamento de ativos do sistema que desempenham papel fundamental aos negócios. Durante o planejamento as maiores dificuldades foram encontradas na escolha de quais empresas iriam compor o estudo, qual delas representaria melhor o tema escolhido. Outra dificuldade encontrada foi na elaboração do questionário para que ele pudesse ser simples, compacto e que abrangesse as informações necessárias para a entrevista e a realização do estudo de caso.

7 CONSIDERAÇÕES FINAIS

A Segurança da Informação é um tema que deve ser tratado seriamente devido aos riscos inerentes as tecnologias que fornecem o suporte aos trabalhos desenvolvidos em diversas empresas. Com a empresa SOLNET esta preocupação ainda é mais importante, pois todos os trabalhos desenvolvidos pela empresa necessitam de uma política de Segurança da Informação.

O presente trabalho forneceu base teórica nos Fundamentos de Segurança da Informação, avaliando os conceitos principais que precisam guiar qualquer iniciativa na área. As principais vulnerabilidades que podem ser exploradas foram mostradas, juntamente com outros conceitos que fornecem embasamento teórico aos interessados no assunto.

É fácil compreender a importância que a Segurança da Informação tem para as empresas atualmente. Muitas informações são conseguidas através do armazenamento de dados nos dispositivos de rede da empresa e fazem parte das atividades necessárias ao seu objetivo, por isso, aplicar uma política de segurança é tarefa administrativa de nível estratégico, que por se utilizar de bens de natureza técnica, deve contar com um grupo com membros capazes de levantar a situação atual do ambiente computacional e pensar em uma solução de segurança.

O valor da informação está diretamente ligado à tomada de decisão e ao gerenciamento estratégico do negócio. É muito mais comum medir a importância da informação pelo valor agregado que ela traz aquilo que é mais concreto, mais visível aos olhos. Muitas vezes os gestores não conseguem perceber, no dia-a-dia, o valor da informação, eles só percebem o efetivo valor quando explicitamente precisam da informação.

Com a disseminação da informação, quase todas as organizações passaram a ser automatizadas, inclusive as microempresas, massificando assim o uso da Tecnologia da Informação. No atual cenário não há mínima condição de uma empresa existir sem utilizar algum tipo de sistema computacional. Os órgãos governamentais estão, a cada dia, mais sofisticados, reduzindo o cerco, afim de que todas as informações apresentadas a eles sejam através da internet, por softwares específicos e com assinaturas digitais.

As empresas devem estar alerta para as diversas técnicas de invasão usadas pelos hackers. Podendo, para tanto se valer de ferramentas de segurança lógica: firewall, ferramentas para detecção de vulnerabilidades, criptografia, backup e antivírus, são exemplos destas ferramentas.

A maior parte das empresas não investe significativamente em Segurança da Informação por considerar como uma questão secundária, mesmo ciente de que esta segurança é importante. A SOLNET afirma que abordar esse assunto geraria um alto custo sem previsão de retorno financeiro. Constatou-se que boa parte dos funcionários entrevistados ainda considera a Segurança de Informação como algo em segundo plano, apesar da maioria concordar que é de grande importância.

Ciente de que este trabalho alcançou a proposta inicialmente mostrando o atual valor da informação e a necessidade do uso das tecnologias da informação, deixa-se como sugestão, para estudos futuros, uma pesquisa complementar a esta com outras empresas para assim identificar e analisar com maior exatidão as possíveis razões do por que as companhias, mesmo sabendo da importância da Segurança da Informação e de seus ativos de rede muitas vezes tomam atitudes omissas em relação à proteção de suas informações.

REFÊRENCIAS

ABNT – Associação Brasileira de Normas Técnicas. **Tecnologia da Informação – Sistemas de Gestão de Segurança da Informação. NBR ISO/IEC 27001**. 30/04/2010.

ABNT – Associação Brasileira de Normas Técnicas. **Tecnologia da Informação – Código de prática para a gestão da segurança da informação. NBR ISO/IEC 17799**. 30/09/2009.

CARNEIRO, Alberto, (2002), **Introdução à Segurança dos Sistemas de Informação, Segurança um fator de sucesso** – Auditoria, Políticas e Benefícios da Segurança, Lisboa, FCA – Editora de informática. ISBN: 972-722-315-X;

DIOGO, D.K.; G.P.L., **Paradigmas de segurança em sistemas operacionais**, UECG, Laboratório de Administração e Segurança de Sistemas, 2004.

DUMONT, Carlos. **Segurança Computacional – Segurança em Servidores Linux em Camadas.** UFLA, 2006.

FONTES, Edison. **Segurança da Informação**. 2001.

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática**. Brasport, 2006.

KAMINSKI, Omar. **Aspectos Jurídicos Relacionados à Segurança da Informação**. III SegInfo – Workshop de Segurança da Informação, 2007.

MARINHO, Eliana; SANTOS, Leandro. **Uma Proposta de Política de Segurança em Redes Linux.** Faculdade Salesiana de Vitória, 2007.

MEDEIROS, João Bosco. Redação **Científica: a prática de fichamentos, resumos, resenhas**. 11. Ed. São Paulo: Atlas, 2010.

MESSMER, E. **Negligência é maior causa de perda ou roubo de informações.** Revista CIO. Disponível em: < http://cio.uol.com.br/>. Acesso em: 28 out. 2012.

MITINICK, Kevin D. **A ARTE DE ENGANAR**. São Paulo: Pearson Educacion do Brasil, 2003.

MOREIRA, N. S. **Segurança mínima – uma visão corporativa da segurança de informações.** Rio de Janeiro: Axcel Books do Brasil, 2001.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec, 2007.

OLIVEIRA, Salomão. **Vírus: Agentes Digitais do Crime**. Evidencia Digital Magazine. Edição 2, 2004.

PEIXOTO, Mário César Pintaudi **Engenharia social e Segurança da Informação** 1.ed.SP: Brasport, 2006.

RAMOS, Anderson. **Conscientização de usuários e Segurança da Informação**. Disponível em <http://www.modulo.com.br >Acesso em 10 de outubro 2012.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**. Rio de Janeiro: Campus, 2003.

SÊMOLA, M. **Roubaram o notebook do funcionário, e agora?** Disponível em: <http://www.semola.com.br>. Acesso em: 01 nov. 2012.

SILVA, C. C. R. Elcelina, (2005), **Perfil de Utilizador em Redes Locais**, monografia de Bacharelato, publicada, Universidade Jean Piaget de Cabo Verde.

SOARES, Luiz Fernando Gomes Et Al. **Redes de Computadores** - das LANS, MANS e WANS às redes ATM. 2°.Ed. - Rio de Janeiro: Editor Campus, 1995.

SOUSA, B. Lindeberg, (2006), **TCP/IP Básico Conectividade em Redes**, Dados, 3ª Edição, Editora Érica Ltda.

STOLLENWERK, Maria Fátima Ludovico. **Gestão do Conhecimento: conceitos e modelos**. In: INTELIGENCIA organizacional e competitiva. Brasília, DF: UNB, 2001.

TANENBAUM, Andrew S. **Redes de Computadores**. 3. ed. RJ: Campus, 1997.

TECNOLOGIA. Podium. **Como anda a segurança da informação nas empresas?** Disponível em: <http://www.podium.com.br/>. Acesso em: 10 nov. 2012.

VASCONCELOS, Fernando Antonio de. **Internet: Responsabilidade do provedor pelos danos praticados**. Jaruá Editora (2003).

ANEXOS

ANEXO A - PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO

INFORMAÇÕES DA SOLNET

1. Nome da organização:
2. Cidade Onde se Localiza:
3. Ano de criação: / /
4. Número de Funcionários:
( ) até 19
( ) de 20 a 99
( ) de 100 a 499

5. O departamento de segurança da SOLNET é:
( ) Próprio da Empresa
( ) Terceirizado
( ) Não Existe

6. No caso de ser próprio, o número de funcionários do departamento é:
( ) Até 5
( ) De 6 a 10
( ) De 11 a 20
( ) Mais de 20

INFORMAÇÕES SOBRE A CONSCIÊNCIA DA SOLNET SOBRE SEGURANÇA

7. Investimento na área de segurança em 2012 é:
( ) Análise de Riscos
( ) Autoridade Certificadora
( ) Biometria
( ) Capacitação da Equipe Técnica
( ) Certificado Digital
( ) Contratação de Empresas Especializadas
( ) Controle de Conteúdo
( ) Criptografia

( ) Implementação de Firewall
( ) Política de Segurança
( ) Sala Cofre/Contra Incêndio
( ) Segurança em Acesso Remoto
( ) Segurança em Internet
( ) Smartcard
( ) Software de Controle de Acesso
( ) Testes de Invasão
( ) Outros:

8. Principais obstáculos para implementação de segurança:
( ) Consciência dos Funcionários
( ) Falta de Apoio Especializado
( ) Ferramentas
( ) Gerência/Diretoria
( ) Orçamento
( ) Outros:

9. Expectativas quanto aos problemas de segurança para 2013:
( ) Aumentarão
( ) Diminuirão
( ) Permanecerão os Mesmos

10. Política de segurança:
( ) Existe e está atualizada
( ) Existe, mas está desatualizada
( ) Não existe

11 . Se existe uma política de segurança, quais os principais tópicos abordados nela:
( ) Análise de Riscos
( ) Cadastro de Usuários
( ) Classificação de Informações
( ) Conceitos Gerais
( ) Cultura de Segurança

( ) Recuperação no caso de Contingências

( ) Segurança Física

( ) Uso da Internet

( ) Uso de Notebooks

( ) Uso de Senhas

( ) Uso de Software

( ) Vírus

( ) Outros:

INFORMAÇÕES SOBRE FALHAS DE SEGURANÇA

12. Principais Ameaças:

( ) Acessos Indevidos

( ) Alteração Indevida

( ) Alteração Indevida de Configurações

( ) Divulgação de Senhas

( ) Divulgação Indevida

( ) Falhas na Segurança Física

( ) Fraudes, Erros e Acidentes

( ) Fraudes em E-mails

( ) Funcionários Insatisfeitos

( ) Hackers

( ) Incêndio/Desastre

( ) Pirataria

( ) Roubo de Senhas

( ) Roubo/Furto

( ) Sabotagens

( ) Super Poderes de Acesso

( ) Uso de Notebooks

( ) Uso Indevido de Recursos

( ) Vazamento de Informações

( ) Vírus

( ) Outras:

13. Principais pontos de invasão:

( ) Internet

( ) Invasão Física

( ) Sistemas Internos

( ) Engenharia Social

( ) Outros:

14. Ataques

( ) Já Sofreu Algum

( ) Nunca Sofreu

( ) Não Sabe se Sofreu

15. Se já sofreu algum tipo de ataque, qual o último registro:

( ) Menos de 1 Mês

( ) De 1 a 6 Meses

( ) De 7 a 12 Meses

( ) De 1 a 2 Anos

( ) Mais de 2 Anos

16. Responsáveis por problemas de segurança registrados:

( ) Internos

( ) Externos

17. Responsáveis por problemas de segurança registrados:

( ) Causa Desconhecida

( ) Vírus

( ) Funcionários

( ) Hackers

( ) Prestadores de Serviços

( ) Outros:

18. Providências adotadas no caso de alguma falha de segurança:

( ) Apenas a Correção dos Problemas

( ) Nenhuma Providência

( ) Providências Internas

( ) Providências Legais

19. Plano de continuidade em caso de falhas de segurança:

( ) Existe

( ) Não Existe

( ) Não Sabe Se Existe

20. Medidas de segurança já implementadas:

( ) Análise Ataques

( ) Análise de Riscos

( ) Assinatura Digital

( ) Autoridade Certificadora

( ) Capacitação e Treinamento

( ) Certificação Digital

( ) Classificação das Informações

( ) Cofre Anti-Incêndio

( ) Contratação de Empresas Especializadas

( ) Controle de Conteúdo

( ) Criptografia

( ) Firewall

( ) Monitoração de Log

( ) Palestras para Usuários

( ) Plano de Continuidade de Negócios

( ) Política de Segurança

( ) Prevenção contra Pirataria

( ) Prevenção contra Vírus

( ) Procedimentos Formalizados

( ) Segurança em Internet

( ) Segurança na Sala dos Servidores

( ) Sistemas de Backup

( ) Sistemas de Detecção de Intrusos

( ) Sistemas de Gestão de Segurança Centralizada

( ) Smartcard

( ) Software de Auditoria
( ) Software de Controle de Acesso
( ) Software de Segurança de Estação
( ) Termo de Responsabilidade
( ) Testes de Invasão

21. Uso corporativo da Internet:
( ) Acesso através da rede da empresa
( ) Acesso via modem na empresa
( ) Acesso via modem na residência
( ) A empresa possui página na Web
( ) É permitido comprar via Internet
( ) Não é permitido usar na empresa
( ) Usa apenas correio eletrônico
( ) Utiliza Internet Banking

23. A SOLNET utiliza a Internet para transações eletrônicas:
( ) Não
( ) Sim

24. Principais aplicações efetuadas na Intranet:
( ) Biblioteca
( ) Certificação Digital
( ) Consultas a Cadastro/Banco de Dados
( ) Corporativos com Manuais e Procedimentos
( ) Divulgação de Documentos e Informativos
( ) Funções Administrativas
( ) HelpDesk
( ) Projetos
( ) Relatórios Internos
( ) RH
( ) Segurança Patrimonial
( ) Sistema de Gestão Empresarial
( ) Sistema de Informações e Controles

( ) Outras:

25. A empresa permite o uso de Internet:

( ) Não permite

( ) Para todos funcionários

( ) Para todos funcionários em determinados horários

( ) Somente para cargos de chefias

26. Soluções para proteção de documentos na Internet:

( ) Criptografia Integrada a Aplicações

( ) Criptografia Integrada a Serviços de Rede

( ) Produtos Específicos

( ) Tecnologia Proprietária

( ) Outras: