UNIVERSIDADE FEDERAL DO PARÁ
CURSO DE SISTEMAS DE INFORMAÇÃO
Campus Marabá

UM ESTUDO DAS PRINCIPAIS FORMAS DE INVASÃO E COMO EVITÁ-LAS

Semuel Silva Costa
Marina Mayla de A. Rodrigues

MARABÁ

2007

MARABÁ

2007

UNIVERSIDADE FEDERAL DO PARÁ
CURSO DE SISTEMAS DE INFORMAÇÃO
Campus Marabá

UM ESTUDO DAS PRINCIPAIS FORMAS DE INVASÃO E COMO EVITÁ-LAS

Marina Mayla de A. Rodrigues
Semuel Silva Costa

Trabalho de Conclusão de Curso, apresentado à Universidade Federal do Pará, como parte dos requisitos necessários para obtenção do Título de Bacharel em Sistemas de Informação.

Orientador: Prof.ª Msc. Alessandra Mariana dos Santos Oliveira

Ficha Catalográfica

COSTA, Semuel S.; RODRIGUES, Marina Mayla de A. *Segurança da Informação*. Marabá: UFPA, 2007. 35p. (Trabalho de Conclusão de Curso apresentado ao Colegiado do Curso de Bacharelado em Sistemas de Informação da Universidade Federal do Pará).

Palavras-Chaves: Segurança da Informação – Vírus – Certificação Digital

AGRADECIMENTOS

Agradeço aos meus pais e todos os meus familiares, pelo apoio, aos meus amigos pela força sempre que necessitei. A todos que direta ou indiretamente contribuíram para que este momento se realizasse, agradeço também ao prof. Ivaldo que sempre nos ajudou e incentivou.

Marina Mayla de Aquino Rodrigues

Agradeço a Deus, aos meus pais pelo esforço, aos amigos que em Marabá contribuíram de forma direta ou indireta para minha formação, aos Professores (as) Raunita Elias Brandão, Mara Rita Duarte de Oliveira e Erivan Sousa Cruz e Ivaldo Horrana, que contribuíram de forma especial para minha formação profissional, acadêmica e pessoal; aos meus tios, que me deram um local para morar enquanto estudante de graduação em Marabá.

Semuel Silva Costa

RESUMO

Com o avanço da tecnologia e a maior aplicabilidade das redes de computadores em nosso cotidiano, surge à necessidade cada dia maior, de se preocupar com a integridade das informações, que circulam no meio computacional das organizações. È realidade dizer que existem mais usuários conectados as redes de computadores e, por esse motivo, é maior a exposição das informações, tornando-se necessário que seja investido recursos em tecnologias de segurança, como equipamentos que garantam a confiabilidade dos negócios, porém mesmo com esses equipamentos ainda não se pode afirmar que é eficaz a segurança da informação. Este trabalho se propõe citar métodos e ferramentas que venham minimizar a possibilidade de invasão por intrusos, que possam tentar se apossar dessas informações de maneira ilegal, para os mais diversos objetivos, que vão da alteração de seu conteúdo original a utilização indevida e até mesmo a destruição total das mesmas, o que pode causar prejuízos irrecuperáveis as organizações.

Palavras-Chaves: Segurança da Informação – Vírus – Certificação Digital.

ABSTRACT

With the advance of the technology and the biggest applicability of the computer networks in our daily one, each bigger day appears to the necessity, of if to worry about the integrity of the information, that circulate in the computational way them organizations, is reality to say that they exist more using connected the computer networks, and for this reason the exposition of the information is bigger, becoming necessary that it is invested resources in security technologies, as equipment that guarantees the trustworthiness of the businesses, however exactly with these equipment not yet if it can affirm that the security of the information is efficient. This work if consider to cite methods and tools that come to minimize the possibility of invasion for intruders, who can try to possess themselves of these information in illegal way, for the most diverse objectives, that even though go of the alteration of its original content the improper use and the total destruction of the same ones, what it can cause irretrievable damages the organizations.

Key-Words: Security of the Information - Virus - Digital Certification.

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

1.1 Considerações Iniciais

Este trabalho tem como tema principal a Segurança da Informação, que torna-se imprescindível na sociedade atual, devido ao grande aumento das redes computacionais na resolução de problemas do cotidiano das organizações. O objetivo deste trabalho, portanto, consiste em demonstrar técnicas de implementação da Segurança da Informação, que vão desde a construção de muros ao redor das organizações até a implementação de softwares que possam detectar e, quando possível, encontrar o responsável por uma possível fraude nos ambientes computacionais. Para o completo desenvolvimento do tema proposto, este estudo foi subdividido em tópicos, considerados mais relevantes, que são: segurança da informação, principais formas possíveis de ameaças existentes em um ambiente computacional, formas de prevenção desse ataques e ferramentas para minimizar a ação dos mesmos.

1.2 Objetivos

Este trabalho propõe um estudo sobre as mais diversas formas de ataques que podem ameaçar a integridade das informações, assim como mostrar as possíveis soluções que podem ser aplicadas contra essas ameaças, com a intenção de minimizar a probabilidade de uma possível invasão em um ambiente computacional.

1.3 Justificativa

Com o grande avanço da implementação das tecnologias no cotidiano das sociedades, surge uma grande gama de novos profissionais da área de Tecnologia da Informação (TI). Em decorrência desse avanço, que proporcionou o surgimento de novas tecnologias e permitiram o transporte da grande quantidade de informações que circulam nos ambientes organizacionais e através da internet, esta nova conjuntura fez com que surgissem vários tipos de usuários, dentre eles podem ser destacados os usuários comuns, os profissionais de TI e, entre essas duas classes, os usuários que desenvolvem softwares mal-intencionados. Esta última classe possui intuitos da mais variada natureza, podendo ir desde a simples interceptação de informações que não lhe pertencem, passando por um possível mau uso das mesmas, sem a autorização dos verdadeiros donos, chegando muitas vezes ao extremo de até mesmo destruí-las, gerando assim não só um grande prejuízo para as organizações,

como também uma terrível incerteza por parte dos usuários, que muitas vezes precisam colocar informações pessoais em ambientes computacionais. Informações tais como senhas de banco, números pessoais de identificação e até mesmo resultados de pesquisas científicas, das mais variadas áreas das ciências, não possuem a certeza de que estejam realmente seguras. Este trabalho propõe, então, demonstrar metodologias que possibilitem a maior segurança das informações na atual conjuntura social.

1.4 Metodologia

Para se abranger um tema com tamanha amplitude, como a área de segurança de informação, será necessário um aprofundamento em pesquisas que envolvem várias subáreas da Tecnologia da Informação em ambientes computacionais, devendo-se buscar a maior fundamentação teórica possível para desenvolver tal pesquisa. Para atingir esse objetivo, foram seguidas as seguintes etapas:

- Busca profunda de conhecimento adquirido ao longo da vida profissional e acadêmica;
- Pesquisa bibliográfica em livros, artigos e trabalhos científicos;
- Pesquisas em sites especializados na área de Segurança da Informação.

1.5 Descrição do Trabalho

O presente trabalho está dividido nos cinco tópicos.

O primeiro tópico é a parte de introdução do trabalho, onde serão descritos os objetivos, a justificativa e a metodologia utilizada.

O segundo tópico mostra o que é segurança da informação e descreve as principais formas de ameaças aos ambientes computacionais.

O terceiro tópico aborda as possíveis formas de prevenção desse ataques e mostra várias ferramentas para minimizar a ação dos mesmos.

O quarto tópico aborda sobre a certificação digital, que utiliza a criptografia e assinatura digital para garantir a autoria e integridade em documentos eletrônicos.

O quinto tópico refere-se a conclusão do trabalho como um todo.

E, por fim, as referencias bibliográficas no sexto tópico.

2 FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO

2.1 Considerações Iniciais

A segurança é um assunto abrangente e inclui um grande número de formas de se cometer irregularidades e, na realidade, se preocupa em evitar com que pessoas não autorizadas tenham acesso a informações que não lhes pertencem, com intuito de utilizá-las de maneira irregular.

A Segurança da Informação nas organizações passa por uma relação considerável de normas que regem os comportamentos de seu público interno e suas próprias atitudes em relação ao público externo e, como ponto forte, consideram-se as ferramentas de hardware e software utilizadas e o domínio da aplicabilidade das mesmas pela organização.

A segurança da informação consiste na preservação dos seguintes atributos:

- Confidencialidade - garantia de que a informação é acessível somente por pessoas autorizadas;
- Integridade - garantia de que as informações e métodos de processamento somente sejam alterados através de ações planejadas e autorizadas;
- Disponibilidade - garantia de que os usuários autorizados tenham acesso à informação e aos ativos correspondentes quando necessário;
- Conforme o caso, também pode ser fundamental para garantir a segurança da informação:
- Autenticidade - garantia da identidade da origem e do destinatário de uma informação.
- Não repúdio - garantia de que o emissor não negará um procedimento por ele realizado.

2.2 Principais Formas de Intrusão

Para se garantir a proteção de uma rede ou sistema é importante conhecer as ameaças e técnicas de ataque utilizadas pelos invasores, para então aplicar as medidas e ferramentas necessárias para proteção desses recursos.

Sem o conhecimento desses fatores, toda a aplicação de mecanismos de proteção pode ser anulada, pois se existir algum ponto vulnerável ou protegido de maneira incorreta, todo o sistema estará comprometido.

Dessa maneira, esta seção busca identificar as principais ameaças e técnicas de ataque contra a segurança da informação.

2.2.1 Sniffers (Farejadores)

Os programas responsáveis por capturar os pacotes de rede são chamados Sniffers, Farejadores ou ainda Capturadores de Pacote. Eles exploram o fato do tráfego dos pacotes das aplicações TCP/IP não utilizar nenhum tipo de cifragem nos dados. Dessa maneira um sniffer pode obter nomes de usuários, senhas ou qualquer outra informação transmitida que não esteja criptografada.

A dificuldade no uso de um sniffer é que o atacante precisa instalar o programa em algum ponto estratégico da rede, como entre duas máquinas, ou em uma rede local com a interface de rede em modo promíscuo.

2.2.2 Spoofing (Falsificação de Endereço)

ANONYMOUS (1999:272) define spoofing como sendo uma técnica utilizada por invasores para conseguirem se autenticar a serviços, ou a outras máquinas, falsificando o seu endereço de origem. Também pode ser definida como uma técnica de ataque contra a autenticidade, através de uma forma de personificação que consiste em um usuário externo assumir a identidade de um usuário ou computador interno, atuando no seu lugar legítimo.

A técnica de spoofing pode ser utilizada para acessar serviços que são controlados apenas pelo endereço de rede de origem da entidade que irá acessar o recurso específico, como também para evitar que o endereço real de um atacante seja reconhecido durante uma tentativa da invasão.

Essa técnica é utilizada constantemente pelos Hackers, sendo que existem várias ferramentas que facilitam o processo de geração de pacotes de rede com endereços falsos.

2.2.3 DoS (Denial-of-Service)

Ter as informações acessíveis e prontas para uso representa um objetivo crítico para muitas organizações. No entanto, existem ataques de negação de serviços (DoS - Denial-of-Service Attack), onde o acesso a um sistema ou determinada aplicação é interrompido ou

impedido, deixando de estar disponível, ou uma aplicação, cujo tempo de execução é crítico, é atrasada ou abortada.

Esse tipo de ataque é um dos mais fáceis de implementar e mais difíceis de se evitar. Geralmente usam spoofing para esconder o endereço de origem do ataque. O objetivo é incapacitar um servidor, uma estação ou tipo de serviço fornecido para os usuários legítimos. Normalmente o ataque DoS não permite o acesso ou modificação de dados. Usualmente o atacante somente quer inabilitar o uso de um serviço e não corrompê-lo.

De acordo com (LIMA, 2000), podem ser destacadas algumas das formas para realização de ataques de negação de serviço:

- *Flooding* - O atacante envia muitos pacotes de rede em curto período de tempo, de forma que a máquina vítima fique sobrecarregada e comece a descartar pacotes (negar serviços);
- *Buffer Overflow* - Uma máquina pode negar serviços se algum software ou sistema operacional tiver alguma falha com o processo de alocação de memória e com o limitado tamanho dos buffers usados. Existem ataques que exploram estes problemas de implementação para, inclusive, rodar código executável remotamente na máquina vítima;
- Pacotes Anormais - Algumas implementações do protocolo TCP/IP não consideram o recebimento de pacotes com formato dos seus dados de maneira incorreta, dessa forma muitas vezes é possível até travar completamente uma máquina ou equipamento remoto enviando pacotes com dados inválidos.

Apesar de geralmente não causarem a perda ou roubo de informações, os ataques DoS são extremamente graves. Um sistema indisponível, quando um usuário autorizado necessita dele, pode resultar em perdas tão graves quanto às causadas pela remoção das informações daquele sistema. Ele ataca diretamente o conceito de disponibilidade, ou seja, realiza ações que visem a negação do acesso a um serviço ou informação.

2.2.4 DDoS (Distributed Denial-of-Services Attacks)

Ao longo do anos de 1999 e 2000, diversos sites sobre segurança da informação (como o CERT, SANS e *SecurityFocus*) começaram a anunciar uma nova categoria de ataques de rede que acabou se tornando bastante conhecida: o ataque distribuído. Neste novo enfoque, os ataques não são baseados no uso de um único computador para iniciar um ataque e sim, são utilizados centenas ou até milhares de computadores desprotegidos e ligados na Internet para lançar coordenadamente o ataque. A tecnologia distribuída não é completamente

nova, no entanto, vem amadurecendo e se sofisticando de tal forma que até mesmo vândalos curiosos e sem muito conhecimento técnico podem causar danos sérios.

Seguindo na mesma linha de raciocínio, os ataques *Distributed Denial of Service* nada mais são do que o resultado de se conjugar os dois conceitos: negação de serviço e intrusão distribuída. Os ataques DDoS podem ser definidos como ataques DoS diferentes partindo de várias origens, disparados simultânea e coordenadamente sobre um ou mais alvos. De uma maneira simples, são ataques DoS em larga escala.

De acordo com (CERT, 2000), os primeiros ataques DDoS documentados surgiram em agosto de 1999, no entanto, esta categoria se firmou como a mais nova ameaça na Internet na semana de 7 a 11 de Fevereiro de 2000, quando vândalos cibernéticos deixaram inoperantes por algumas horas sites como o Yahoo, EBay, Amazon e CNN. Uma semana depois, teve-se notícia de ataques DDoS contra sites brasileiros, tais como: UOL, Globo On e IG, causando com isto uma certa apreensão generalizada.

Para realização de um ataque DDoS são envolvidos os seguintes personagens:

- **Atacante:** Quem efetivamente coordena o ataque;
- ***Master:*** Máquina que recebe os parâmetros para o ataque e comanda os agentes;
- **Agente:** Máquina que efetivamente concretiza o ataque DoS contra uma ou mais vítimas, conforme for especificado pelo atacante. Geralmente um grande número de máquinas que foram invadidas para ser instalado o programa cliente;
- **Vítima:** Alvo do ataque. Máquina que é "inundada" por um volume enorme de pacotes, ocasionando um extremo congestionamento da rede e resultando na paralisação dos serviços oferecidos por ela.

Vale ressaltar que, além destes, existem outros dois personagens atuando nos bastidores:

- ***Daemon:*** Processo que roda no agente, responsável por receber e executar os comandos enviados pelo cliente;
- **Cliente:** Aplicação que reside no *master* e que efetivamente controla os ataques enviando comandos aos *daemons*.

Os ataques DDoS amplificam o poder de ação dos ataques DoS utilizando computadores comprometidos, os agentes, onde os daemons foram instalados indevidamente devido a vulnerabilidades exploradas pelos atacantes. A partir do momento que o master envia o comando de início para os agentes, o ataque à vítima se inicia em grande escala. Esse tipo de ataque mostra como a segurança de qualquer equipamento à Internet é importante, onde qualquer host vulnerável pode ser utilizado como recurso para um ataque.

2.2.5 Ataque de Senhas

Segundo (CLIFF, 2001), a utilização de senhas seguras é um dos pontos fundamentais para uma estratégia efetiva de segurança. As senhas garantem que somente as pessoas autorizadas terão acesso a um sistema ou à rede. Infelizmente isso nem sempre é realidade. As senhas geralmente são criadas e implementadas pelos próprios usuários que utilizam os sistemas ou a rede. Palavras, símbolos ou datas fazem com que as senhas tenham algum significado para os usuários, permitindo que eles possam facilmente lembrá-las. Neste ponto é que existe o problema, pois muitos usuários priorizam a conveniência ao invés da segurança. Como resultado, eles escolhem senhas que são relativamente simples. Enquanto isso permitem que possam lembrar facilmente das senhas e também facilitam o trabalho de quebra dessas senhas por hackers. Em virtude disso, invasores em potencial estão sempre testando as redes e sistemas em busca de falhas para entrar. O modo mais notório e fácil a ser explorado é a utilização de senhas inseguras. A primeira linha de defesa, a utilização de senhas, pode se tornar um dos pontos mais falhos.

Parte da responsabilidade dos administradores de sistemas é garantir que os usuários estejam cientes da necessidade de utilizar senhas seguras. Isto leva a dois objetivos a serem alcançados: primeiro, educar os usuários sobre a importância do uso de senhas seguras; e segundo, implementar medidas que garantam que as senhas escolhidas pelos usuários são efetivamente adequadas. Para alcançar o primeiro objetivo, a educação do usuário é o ponto chave. Já para alcançar o segundo objetivo, é necessário que o administrador de sistemas esteja um passo à frente, descobrindo senhas inseguras antes dos atacantes. Para fazer isso é necessária a utilização das mesmas ferramentas utilizadas pelos atacantes.

(CLIFF, 2001) descreve as duas principais técnicas de ataque a senhas:

- **Ataque de Dicionário:** Nesse tipo de ataque são utilizadas combinações de palavras, frases, letras, números, símbolos, ou qualquer outro tipo de combinação geralmente que possa ser utilizada na criação das senhas pelos usuários. Os programas responsáveis por realizar essa tarefa trabalham com diversas permutações e combinações sobre essas palavras. Quando alguma dessas combinações se referir à senha, ela é considerada como quebrada (*Cracked*). Geralmente as senhas estão armazenadas criptografadas utilizando um sistema de criptografia HASH. Dessa maneira os programas utilizam o mesmo algoritmo de criptografia para comparar as combinações com as senhas armazenadas. Em outras palavras, eles adotam a mesma configuração de criptografia das senhas, e então criptografam as palavras do dicionário e comparam com a senha.

- **Força-Bruta:** Enquanto as listas de palavras, ou dicionários, dão ênfase a velocidade, o segundo método de quebra de senhas se baseia simplesmente na repetição. Força-Bruta é uma forma de se descobrir senhas que compara cada combinação e permutação possível de caracteres até achar a senha. Este é um método muito poderoso para descoberta de senhas, no entanto é extremamente lento porque cada combinação consecutiva de caracteres é comparada.

2.2.6 Vírus, Trojans e Worms

Batizadas genericamente de Malware, essas pragas virtuais têm ganhado espaço nos últimos anos no que diz respeito aos prejuízos encarados por empresas. Como se defender com eficiência contra as pragas é a pergunta que povoa a mente de administradores, gestores de segurança e empresários, cada vez mais preocupados com as perdas que enfrentam ao ingressar nesse admirável mundo novo chamado Internet. Se houvesse apenas uma resposta para essa dúvida, de como aproveitar todos os recursos trazidos pela rede sem sofrer com os riscos, estariam todos satisfeitos. Mas, infelizmente, a experiência mostra que lidar com ameaças virtuais exige uma série de cuidados que não se restringe ao uso de antivírus.

Os vírus são pequenos segmentos de códigos, programados com o intuito de provocar algum sintoma indesejável ao usuário do computador infectado. Possuem a característica de se agregarem ao código de outros programas e, ao serem executados inocentemente pelo usuário, trazem em seu bojo, o código alterado para causar intromissões indevidas no processamento normal, causando ou não, danos de leves a irreparáveis na maquina infectada (CIDALE, 1990).

O código do vírus funciona como uma função de programa que se apodera de áreas importantes de comando do sistema, de onde podem transferir réplicas de seus códigos a outros arquivos já presentes na memória ativa e a arquivos que estejam armazenados nos discos rígidos (CIDALE, 1990).

Esta capacidade de se multiplicar pela contaminação através de arquivos transmitidos por disquetes, cds e outros meios de se compartilhar informações, levou a similaridade e comparação com os vírus biológicos que infectam, por auto-reprodução, diversos órgãos do corpo humano (CIDALE, 1990).

Com o passar do tempo surgiram novas formas de contágio através da rede de computadores que podem ser sub-divididas da seguinte forma:

Malware - O termo malware, é uma abreviatura da expressão "*malicious software*" (software mal-intencionado) e pode ser usado como um substantivo coletivo para se

referir a vírus, vermes e cavalos de tróia que executam deliberadamente ações mal intencionadas em um sistema de computador;

Worms (Verme) - Usa um código mal intencionado e auto propagável que pode se distribuir automaticamente de um computador para outro através das conexões de rede. Um verme pode desempenhar ações nocivas, como consumir recursos da rede ou do sistema local podendo causar um ataque de negação de serviço, ou seja, indisponibilidade;

Trojans (Cavalo de Tróia) - Programa que parece útil ou inofensivo, mas contém códigos ocultos desenvolvidos para explorar ou danificar o sistema o qual é executado. Os Cavalos de Tróia geralmente chegam aos usuários através de mensagens de e-mail que disfarçam a finalidade e função do programa.

2.2.7 Engenharia Social

O termo Engenharia Social é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter acesso a informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Refere-se a essa situação como Engenharia por que através das informações obtidas serão contruídas táticas de acesso a sistemas e informações secretas, de forma indevida. Social por que se utiliza de pessoas.

Os ataques do chamado engenheiro social são direcionados diretamente para o elo mais fraco de qualquer sistema de segurança: as pessoas. Ele utiliza sua criatividade e habilidade, pra envolver a vítima, sendo que esta muitas vezes nem percebe que abriu espaço para um invasor.

A falta de consciência das técnicas de engenharia social utilizadas e o excesso de autoconfiança das pessoas (por não se considerarem ingênuas e acharem que não podem ser manipuladas) são os principais fatores que favorecem ao sucesso da Engenharia Social (SANTOS, 2004).

2.3 Considerações Finais

Através do conhecimento das várias maneiras que os invasores podem se utilizar para invadir um determinado ambiente computacional, seja com o intuito de obter informações pessoais tais como senhas de bancos ou tornar determinado serviço indisponível

a usuários legítimos, nos faz refletir sobre a necessidade de tomar determinadas atitudes de prevenção contra esses ataques.

O próximo capítulo se propõe, então, a demonstrar algumas das maneiras de se detectar, em um sistema, falhas de segurança ou ainda sintomas de que o mesmo tenha sido vítima desse tipo de invasão para corrigi-lo e mantê-lo seguro.

3 PRINCIPAIS FORMAS DE SEGURANÇA

3.1 Considerações Iniciais

Hoje em dia se faz necessário tomar atitudes direcionadas a segurança das informações que circulam nas redes locais das organizações, para enfim se garantir a integridade física e lógica das mesmas, tais como a implementação de firewalls, backup, auditorias, antivírus e outros.

Este capítulo tem como finalidade demonstrar algumas das ações que devem ser implementadas a fim de garantir a integridade das informações nas organizações.

3.2 Segurança Física

O controle de acesso físico visa impedir que pessoas estranhas ao ambiente tenham acesso às dependências, protegendo os equipamentos que tratam ou armazenam as informações, através da implementação de acessos restritos a esses ambientes, buscando a prevenção de possíveis perdas, roubos ou vazamentos de informações. A segurança física tem como principais objetivos: garantir a continuidade das rotinas, assegurar a integridade dos ativos e manter a integridade e confidencialidade das informações.

Medidas de proteção física, tais como serviços de guarda, uso de no-breaks, alarmes e fechaduras, circuito interno de televisão e sistemas de escuta são realmente uma parte da Segurança da Informação, visto que têm um importante papel também na prevenção dos itens citados anteriormente.

O ponto-chave é que as técnicas de proteção de dados, por mais sofisticadas que sejam, não têm serventia nenhuma se a segurança física não for garantida.

3.3 Segurança Lógica

Pode-se entender segurança lógica a maneira de estabelecer os controles de acesso a informação, objetivando a integridade e a manutenção da confidencialidade. Nela definem-se as permissões de acesso a aqueles previamente autorizados e negando o acesso daqueles que não gozem dos mesmo direitos, principalmente em ambientes que concentrem um percentual elevado de informações, como exemplo, as redes de comunicação ou os grandes centros de processamento de informações das organizações.

Quanto maior for a utilização do processamento eletrônico de dados, maior será o aumento de sua vulnerabilidade, sendo desta forma necessária a utilização de meios de segurança mais eficientes para a proteção dos dados manuseados. "O estabelecimento de controles para segurança lógica dos dados deve ser avaliada pelo aspecto custo/benefício..." (FONTES, 1991), pois a redução dos riscos às informações aumenta em contra partida a confiabilidade dos dados, assim como, aumenta a sobrecarga dos computadores, alongando os tempos de resposta e os custos.

3.4 Ferramentas de Segurança Lógica

3.4.1 Firewalls

O firewall é uma barreira inteligente entre duas redes, geralmente a rede local e a Internet, através da qual só passa tráfego autorizado. Este tráfego é examinado pelo firewall em tempo real e a seleção é feita de acordo com um conjunto de regras de acesso. Ele é tipicamente um roteador (equipamento que liga as redes com a lnternet), um computador rodando filtragens de pacotes, um software proxy, um firewall-in-a-box (um hardware proprietário específico para função de firewall) ou um conjunto desses sistemas.

Pode-se dizer que firewall é um conceito ao invés de um produto. Ele é a soma de todas as regras aplicadas a rede. Geralmente, essas regras são elaboradas considerando as políticas de acesso da organização.

De acordo com os mecanismos de funcionamentos dos firewalls podem-se destacar três tipos principais:

- Filtros de pacotes;
- Stateful Firewalls;
- Firewalls em Nível de Aplicação.

Um esboço de representação de um Firewall pode ser visualizado na Figura 3.1, que mostra o posicionamento do mesmo em uma rede e os três tipos principais são descritos sequência.

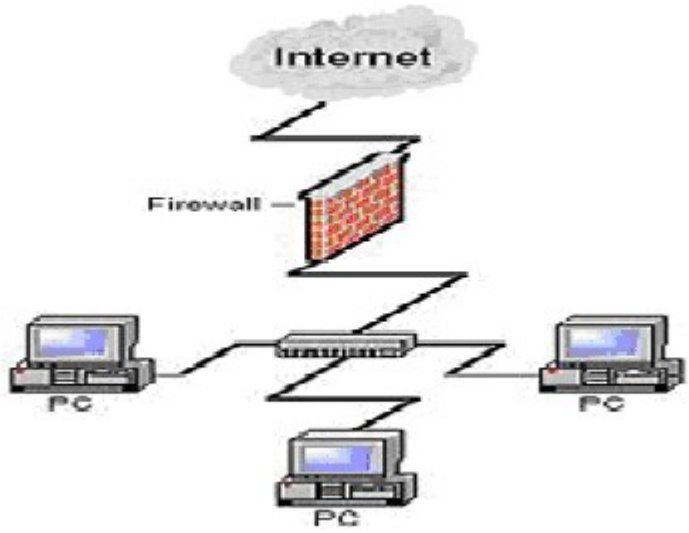

Figura 3.1 – Esquema de Representação de um Firewall
FONTE: Guia Slackware, 2004 (Adaptado)

- **Filtros de Pacotes**

Esse é o tipo de firewall mais conhecido e utilizado. Ele controla a origem e o destino dos pacotes de mensagens da lnternet. Quando uma informação é recebida, o firewall verifica as informações sobre o endereço IP de origem e destino do pacote e compara com uma lista de regras de acesso para determinar se pacote está autorizado ou não a ser repassado através dele.

Atualmente, a filtragem de pacotes é implementada na maioria dos roteadores e é transparente aos usuários, porém pode ser facilmente contornada com IP Spoofers. Por isto, o uso de roteadores como única defesa para uma rede corporativa não é aconselhável.

Mesmo que filtragem de pacotes possa ser feita diretamente no roteador, para uma maior performance e controle, é necessária a utilização de um sistema específico de firewall. Quando um grande número de regras é aplicado diretamente no roteador, ele acaba perdendo performance. Além disso, firewalls mais avançados podem defender a rede contra spoofing e ataques do tipo DoS/DDoS.

- **Stateful Firewalls**

Um outro tipo de firewall é conhecido como *Stateful Firewall*. Ele utiliza uma técnica chamada Stateful Packet Inspection, que é um tipo avançado de filtragem de pacotes. Esse tipo de firewall examina todo o conteúdo de um pacote, não apenas seu cabeçalho, que contém apenas os endereços de origem e destino da informação. Ele é chamado de ‘stateful’

porque examina os conteúdos dos pacotes para determinar qual é o estado da conexão. Por exemplo, ele garante que o computador destino de uma informação tenha realmente solicitado anteriormente a informação através da conexão atual.

Além de serem mais rigorosos na inspeção dos pacotes, os Stateful Firewalls podem ainda manter as portas fechadas até que uma conexão para a porta específica seja requisitada. Isso permite uma maior proteção contra a ameaça de port scanning.

- **Firewalls em Nível de Aplicação**

Nesse tipo de firewall o controle é executado por aplicações específicas, denominadas proxies, para cada tipo de serviço a ser controlado. Essas aplicações interceptam todo o tráfego recebido e o envia para as aplicações correspondentes, assim, cada aplicação pode controlar o uso de um serviço.

Apesar desse tipo de firewall ter uma perda maior de performance, já que ele analisa toda a comunicação utilizando proxies, ele permite uma maior auditoria sobre o controle no tráfego, já que as aplicações específicas podem detalhar melhor os eventos associados a um dado serviço.

A maior dificuldade na sua implementação é a necessidade de instalação e configuração de um proxy para cada aplicação, sendo que algumas aplicações não trabalham corretamente com esses mecanismos.

3.4.2 Sistemas de Detecção de Intrusos

São sistemas inteligentes, capazes de detectar tentativas de invasão em tempo real. Estes sistemas podem apenas alertar sobre a invasão como, também, aplicar ações necessárias contra o ataque. Eles podem ser sistemas baseados em regras ou adaptáveis. No primeiro, as regras de tipos de invasões e a ação a ser tomada são previamente cadastradas. O problema é que a cada dia surgem novos tipos de ataques e estas regras precisam estar sempre atualizadas para o sistema ser realmente eficaz. No segundo tipo, são empregadas técnicas mais avançadas, inclusive de inteligência artificial, para detectarem novos ataques, sempre que surgirem.

3.4.3 Logs e Auditoria

De uma maneira simples, os logs são quaisquer registros, gerados pelo sistema operacional ou aplicações, com informações sobre os eventos ocorridos para uma posterior verificação. Apesar de ser uma medida de segurança básica, muitos esquecem dos arquivos de logs, pois eles são uma das formas mais elementares de auditoria de sistemas.

Os logs são extremamente importantes por três razões principais. Primeira, eles podem fornecer uma visão das atividades que estão ocorrendo nos sistemas. Segunda, eles podem fornecer dados para análises de detecção de problemas ou falhas de segurança nos sistemas. Teceira, talvez a mais importante, os logs podem ser utilizados como evidências de um incidente de segurança.

Os logs podem fornecer informações valiosas, mas que muitas vezes são ignoradas pela falta de tempo para revisar tantas informações. O mais indicado é automatizar o processo de forma que torne mais fácil a verificação dos logs e somente as informações necessárias são extraídas e notificadas. Além desse processo de filtragem podem ser consideradas outras recomendações sobre a utilização dos logs, de acordo com (ALEGRE, 1999):

- Criar uma política de logs séria, identificando: os tipos de informação que podem ser registrados, os mecanismos para tal registro, onde essa tarefa será realizada e onde os arquivos de logs serão armazenados;
- Determinar se os mecanismos providos pelo sistema, e na rede de maneira geral, registram as informações necessárias;
- Habilitar os mecanismos de logs. Recomenda-se em uma primeira instância registrar o máximo de logs possíveis, e posteriormente, determinar que dados são mais significativos dentro de um processo de detecção de intrusão;
- Monitorar os arquivos de logs regularmente em busca de atividades suspeitas;
- Investigar qualquer anomalia encontrada, isto é, verificar que se ela pode ser atribuída a algum tipo de atividade autorizada, por exemplo: o usuário realmente estava em Toronto no dia anterior e conectou-se no sistema? Ou houve realmente uma queda de energia que fez com que o sistema seja reinicializado?
- Caso seja confirmada qualquer evidência (ou tentativa) de intrusão, contactar seu respectivo grupo de segurança e reportar o incidente ou, se este grupo não existir, contatar diretamente os responsáveis técnicos das redes comprometidas.

3.4.4 Antivírus

São pacotes de software que podem checar seu disco rígido HD e suas unidades de armazenamento secundárias quanto à presença de programas não desejados e prejudiciais aos sistemas operacionais, os famosos vírus.

A função principal é proteger a máquina, ou seja, alertar da presença do vírus em um arquivo que por ventura o usuário estiver copiando para sua máquina através de disquetes, cds ou de outras formas já mencionadas anteriormente como arquivos recebidos por e-mail, downloads de programas, musicas MP3 pelas redes P2P, bem como limpar arquivos infectados, deixando os dados originais intactos; no entanto, isto nem sempre é possível, pois alguns vírus causam danos irrecuperáveis. Às vezes, a única forma de se livrar de um arquivo infectado é excluí-lo. Existe uma enorme variedade de fabricantes, entre as principais podemos citar a Mcafee, Trend, Symantec, Panda, entre outros, que são softwares pagos, porém existem fabricantes que fornecem seu produto gratuitamente para uso doméstico como a GRISOFT que fornece o antivírus AVG. Estes produtos oferecem a prevenção e uma série de facilidades para monitorar constantemente as atividades dos arquivos em um computador.

3.4.5 Recuperação de Desastres e Backup

Podemos definir recuperação de desastres como o processo de restauração do sistema após a perda de dados.

ANONYMOUS (1999:553), descreve as principais ameaças que podem causar um desastre a um sistema:

- Força Maior: Ações da Natureza (erupções vulcânicas, incêndios, enchentes, terremotos, furacões ou maremotos) podem acabar totalmente com os equipamentos e, conseqüentemente, com os dados;
- Erros inocentes: Usuários autorizados podem inadvertidamente destruir ou sobrescrever dados vitais enquanto estiverem administrando os sistemas;
- Falhas Mecânicas: Na era do hardware barato, onde ha a produção em massa de hardware, falhas mecânicas são comuns. Um harddisk novo às vezes pode simplesmente falhar, por exemplo;
- Falhas em programas: Algum programa que possua falhas ou erros de programação pode danificar dados importantes.

Essas ameaças, além de vírus, ataques ou qualquer outra atividade maliciosa influenciam diretamente, em vários níveis, na operação de uma empresa, desde uma estação individual até uma rede corporativa inteira. Quando algum desastre aconteçe, ao invés de se descobrir à origem, o foco principal é restaurar os recursos de tecnologia da informação para sua total funcionalidade, restaurando as operações do negócio. Quanto maior for a demora, maiores serão as conseqüências para a empresa.

Backups diários ou semanais dos sistemas, incluindo dados essenciais para operação da empresa, são componentes vitais para restauração de desastres e para manutenção das funções da empresa.

3.5 Considerações Finais

Com a correta utilização dos métodos de segurança anteriormente citados podemos minimizar a possibilidade de se ter a rede atacada por intrusos, porém temos que levar em consideração que no momento que se envia uma informação para outra rede esta pode se tornar vulnerável devido estar em um ambiente externo, onde se torna sujeita a ser capturada por terceiro e utilizada de maneira não autorizadas pelos seus verdadeiros donos. Também precisamos entender que nem sempre as ameaças são provenientes do ambiente externo a rede. Estes são motivos pelo qual se faz necessária à utilização da tecnologia conhecida como Criptografia.

O próximo capítulo busca mostrar, então, o que é, como funciona e quais as vantagens em nível de segurança de se utilizar a criptografia nos ambientes das organizações.

4 CERTIFICAÇÃO DIGITAL

4.1 Considerações Iniciais

A criptografia ou arte de escrever em cifras é, na realidade, uma maneira de se enviar determinada informação codificada (criptografada) para seu destinatário, de forma a garantir que mesmo sendo capturada por terceiros não venha a ser utilizada, por estar inelegível, garantindo assim que somente seu receptor original, ou um receptor que contenha a chave para a decodificação da mesma consiga decifrar e ler seu conteúdo.

Este capítulo busca mostrar as maneiras de se empregar esta tecnologia, que é amplamente utilizada por instituições financeiras, de pesquisa e nos mais variados ramos da ciência.

4.2 Certificação Digital

Atualmente os computadores e a internet são muito utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto este tipo de comunicação deve adotar mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações. A tecnologia que provê estes mecanismos de segurança é a Certificação Digital.

Dentro da certificação digital está o certificado digital, um documento eletrônico que tem como função provar para as pessoas e para os sistemas de informação que você é quem você diz. E junto ao certificado digital, vem o nome da pessoa, um número público, que é denominado chave pública e outros dados. Esta chave pública serve para validar uma assinatura digital em documento eletrônico.

A tecnologia da certificação digital foi desenvolvida graças aos avanços da criptografia nos últimos 30 anos. A palavra criptografia tem origem grega e significa a arte de escrever em códigos. Esse processo de codificação que é feito na informação é chamado de cifragem. O processo inverso é chamado de decifragem.

O certificado não garante que se esteja lidando com alguém respeitável. O que ele realmente significa é que, se alguém for roubado, terá uma chance muito boa de ter um endereço físico e real e alguém para processar.

4.3 Criptografia

Existem dois tipos de criptografia: a simétrica e a de chave pública. A criptografia simétrica garante sigilo na transmissão e armazenamento dos dados, sendo esta realizada pela cifragem e decifragem de uma informação através de algoritmos que utilizam a mesma chave. A chave deve ser compartilhada entre quem cifra e quem decifra os dados. Esse processo de compartilhar uma chave é conhecido como troca de chaves e deve ser feita de forma segura.

A criptografia de chave pública opera com duas chaves distintas, uma pública e uma privada. Essas chaves são geradas simultaneamente e são relacionadas entre si. A vantagem é que a chave pública pode ser distribuída publicamente, ou seja, qualquer pessoa para quem você forneça sua chave pública pode enviar uma mensagem segura, contanto que somente você tenha sua chave privada.

Um esquema de Criptografia de Chave Pública pode ser se visto através da figura a seguir.

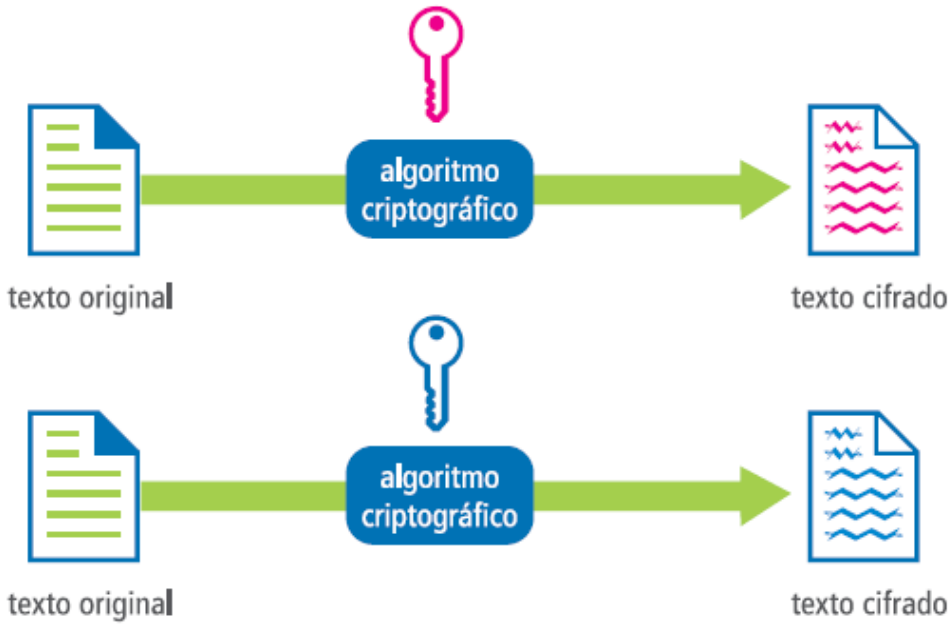

Figura 4.1 – Esquema de criptografia
FONTE: Curso de Segurança em Redes - UFF

4.3.1 Algoritmos criptográficos de chave pública ou assimétrica

Os algoritmos de chave pública permitem garantir tanto a confidencialidade quanto a autenticidade das informações por eles protegidas.

- **Confidencialidade**

Para que o emissor envie uma informação sigilosa, ele deve utilizar a chave publica do destinatário, sendo que este deve disponibilizar sua chave publica em diretórios públicos acessíveis pela internet.

Através da figura abaixo é possível termos um melhor entendimento de como é utilizada a chave pública e a chave privada a fim de se garantir a Confidencialidade.

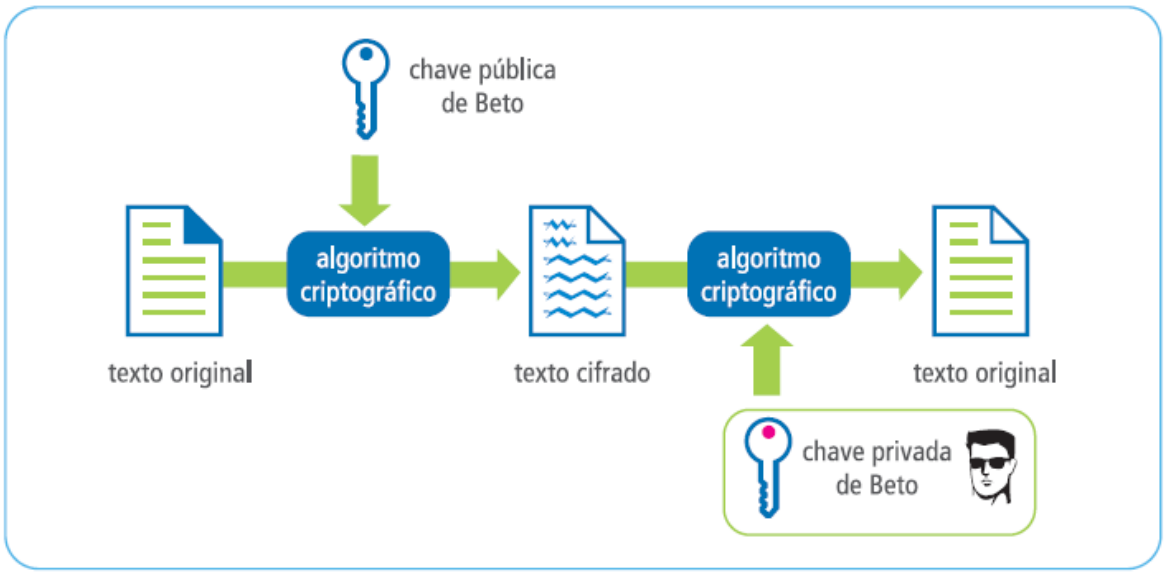

Figura 4.2 – Esquema de criptografia – Chave Pública
FONTE: Curso de Segurança em Redes - UFF

O sigilo é garantido, já que somente o destinatário que possui a chave privada conseguirá desfazer a operação de cifragem, ou seja, decifrar e recuperar as informações originais. Por exemplo, para Alice compartilhar uma informação de forma secreta com Beto, ela deve cifrar a informação usando a chave pública de Beto. Somente Beto pode decifrar a informação, pois somente Beto possui a chave privada correspondente.

- **Autenticidade**

No processo de autenticação, as chaves são aplicadas no sentido inverso ao da confidencialidade.

O autor de um documento utiliza sua chave privada para cifrá-lo de modo a garantir a autoria em um documento ou a identificação em uma transação. Esse resultado só é obtido porque a chave privada é conhecida exclusivamente por seu proprietário.

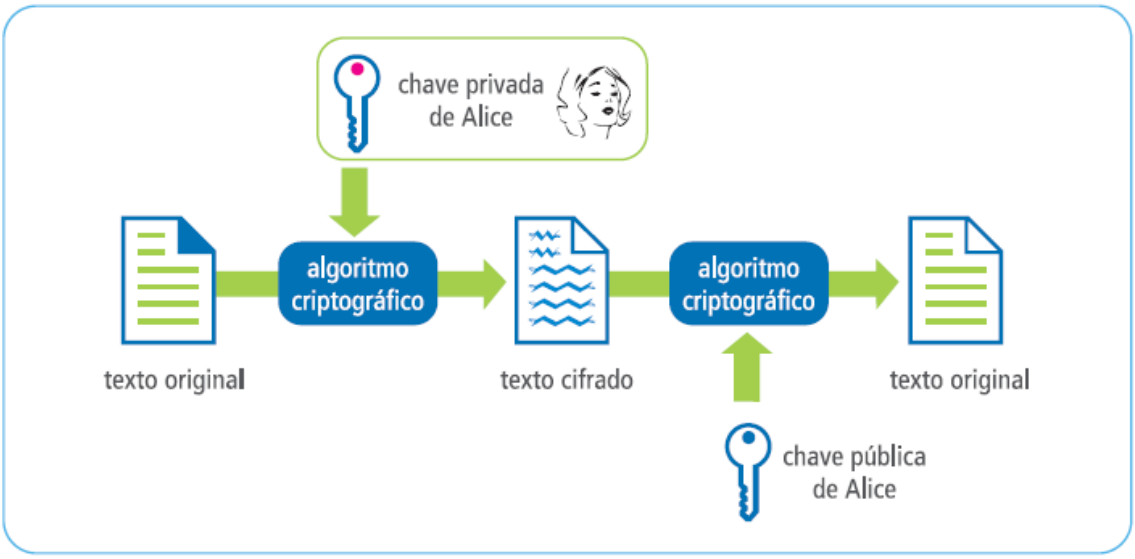

Figura 4.3 – Esquema de criptografia – Chave Privada
FONTE: Curso de Segurança em Redes - UFF

Assim, se Alice cifrar uma informação com sua chave privada e enviar para Beto, ele poderá decifrar esta informação, pois tem acesso à chave pública de Alice. Além disto, qualquer pessoa poderá decifrar a informação, uma vez que todos conhecem a chave pública de Alice. Por outro lado, o fato de ser necessário o uso da chave privada de Alice para produzir o texto cifrado caracteriza uma operação que somente Alice tem condições de realizar.

4.4 Assinatura Digital

O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de hash, é chamada de assinatura digital.

Figura 4.4 – Esquema de criptografia com *hash*
FONTE: Curso de Segurança em Redes - UFF

O resumo criptográfico é o resultado retornado por uma função de *hash*. Este pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

Através desta ilustração podemos ver como a função de *hash* é empregada na criação do resumo criptográfico.

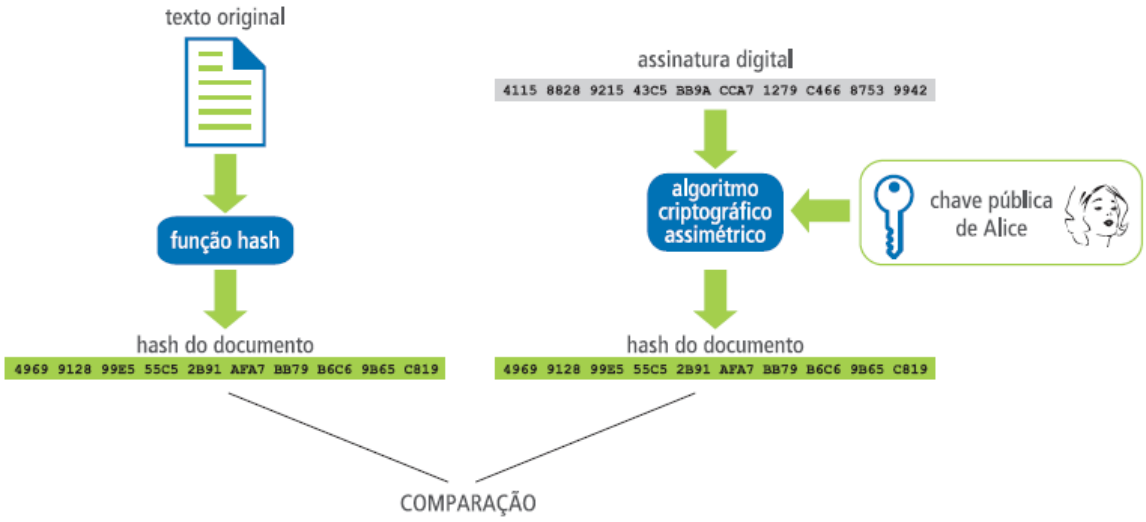

Figura 4.5– Esquema de assinatura digital
FONTE: Curso de segurança em Redes - UFF

Para comprovar uma assinatura digital é necessário inicialmente efetivar duas operações: é realizado um cálculo do resumo criptográfico do documento e então é decifrada a assinatura com a chave pública do signatário. Se forem iguais, significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro, ou seja, a assinatura está correta. Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura pública.

A Assinatura Digital é hoje a forma mais eficaz de garantir autoria de documentos eletrônicos. Em 2001, ela passou a ter validade jurídica, garantindo a utilização de certificados digitais.

4.5 Certificado Digital

O Certificado Digital é um documento eletrônico assinado digitalmente que cumpre a função de associar uma pessoa ou entidade a uma chave pública.

Um Certificado Digital normalmente apresenta as seguintes informações:

- nome da pessoa ou entidade a ser associada à chave pública;
- período de validade do certificado;
- chave pública;
- nome e assinatura da entidade que assinou o certificado;
- número de série.

Por exemplo, os serviços bancários via internet utilizam o certificado para garantir junto ao cliente que o acesso está realmente ocorrendo com o servidor. O governo também se estruturou para suportar transações eletrônicas, visando benefícios para os cidadãos e também proporcionando uma maior satisfação do usuário, entre outros.

Autoridade Certificadora (AC) é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais. Entre as atividades de uma AC, a mais importante é verificar a identidade da pessoa ou da entidade antes da emissão do certificado digital. O certificado digital emitido deve conter informações confiáveis que permitam a verificação da identidade do seu titular. Por estes motivos, quanto melhor definidos e mais abrangentes os procedimentos adotados por uma AC, maior será sua confiabilidade.

4.6 Considerações Finais

Com a implementação das técnicas de criptografia e certificação digital anteriormente citadas, podemos ter maior confiabilidade na integridade das informações que circulam tanto nas redes locais como em ambientes externos. Graças a estas tecnologias é que hoje se vê um grande número de transações financeiras sendo realizadas a distância, .possibilitando a maior comodidade e segurança para milhares de usuários distribuídos pelo

mundo inteiro, visto que, a maioria das informações que trafegam nas redes computacionais são de extrema confidencialidade, tanto para as organizações quanto para seus clientes.

5 CONCLUSÃO

Com o acesso às redes de computadores e com o número cada vez maior de pessoas conectadas entre si, houve a necessidade de criação de novos conceitos, dentre esses conceitos a palavra segurança tem se tornado cada dia mais comum em nosso cotidiano, pois ao se conectar em uma rede estamos propensos a determinados riscos e perda de nossas informações pessoais.

Como uma constatação desse fato, atualmente empresas que tem áreas em seu *site* destinadas a clientes tem adotado medidas de prevenção contra possíveis ataques que possam deixar duvidosa a integridade e a confiabilidade do sistema, e para que estas tenham maior segurança das informações nesse ambiente, adotam técnicas de segurança como medidas de prevenção. Assim como a utilização de firewalls e análise de logs a fim de manter um ambiente o mais seguro possível.

Contudo pode-se citar a certificação digital como uma das mais usadas formas de prevenção contra invasores, pois ao mesmo tempo que impede os ataques, protege a informação de qualquer tentativa de acesso, dano, violação ou até mesmo alteração de conteúdos.

Por isso no mundo atual onde a palavra segurança tem se tornado cada vez mais um assunto delicado e importante dentro de empresas e até em aplicações por essas utilizadas, tanto conceitos bem como ações praticas da segurança estão se tornando a nova tendência da computação moderna. Logo as tecnologias que surgem tendem a dar uma maior ênfase a essa pratica, por essa ser de grande importância para a proteção das informações.

REFERÊNCIAS BIBLIOGRÁFICAS

RICCI, Bruno. **Slackware – Guia Pratico**. Ed. Ciência Moderna, 2004.

ALEGRE, Liliana Esther Velásquez. **Os Logs como Ferramenta de Detecção de Intrusão**, 1999. Disponivel em: http://www. rnp. br/. Acessado em: 29 jan. 2007.

ANONYMOUS. **Maximum Linux Security.** Estados Unidos — Indianapolis: Sams, 1999. Disponivel em: http://www.projetosderedes.kit.net. Acessado em: 20 dez. 2006.

CAMPELLO, Rafael et al. **Anais do WSEG'2001: Workshop em Segurança de Sistemas Computacionais** 2001. Porto Alegre: SBC, 2001. Disponível em: http://www.projetosderedes.kit.net. Acessado em: 20 jan. 2006.

CERT Coordination Center, Disponivel em: http://www.cert.org. Acessado em: 13 jan. 2007.

CIDALE, Ricardo A. **Vírus digital. Uma abordagem para prevenção e manutenção de seus sistemas de informação**. São Paulo: Makron McGraw-Hill, 1990. Disponível em: http://http.modulo.com.br/. Acessado em: 01 fev. 2007

CLIFF, A. **Password Crackers — Ensuring the Security of Your Password,** 2003. Disponivel em: http://www.securityfocus.com/. Acessado em: 16 jan. 2007.

FONTES, Edison. **Política da Segurança da Informação,** 2005. Disponivel em: http://www.modulo.com.br/. Acessado em: 10 jan. 2007.

LIMA, Marcelo B. **Firewalls — Uma Introdução à Segurança.** Revista do **Linux.** Curitiba, 2000. Disponivel em: http://www.projetosderedes.kit.net. Acessado em: 20 dez. 2006.

MEDEIROS, Carlos Diego Russo. **Segurança da Informação: Implantação de medidas e ferramentas de Segurança da Informação**, 2001. Disponível em: http://www.projetoderedes.kit.net/. Acessado em: 14 de dez. 2006.

NORMA NBR ISO/IEC 17799. **Código de Prática para Gestão da Segurança da Informação nas Empresas**. ABNT – Associação Brasileira de Normas. Disponível em: http://www.modulo.com.br/. Acessado em: 02 fev. 2007.

PANETTA, Nelson. **Criptografia**. **Security Magazine.** São Paulo, 2000. Disponivel em: http://www.projetosderedes.kit.net/artigos. Acessado em: 20 dez. 2006.

SANTOS, Luciano Alves Luguinho**. O Impacto da Engenharia Social na Segurança da Informação,** 2004. Disponível em: http://www.modulo.com.br/. Acessado em: 19 de jan. 2007.

SILVA, João Pedro da. **Evolução das pragas virtuais,** 2005. Disponível em: http://www.modulo.com.br/. Acessado em: 19 de jan. 2007.