www4.fsanet.com.br/revista
Revista Inova Ação, Teresina, v. 1, n. 2, art. 6, p. 77-88, jul./dez. 2012
ISSN Impresso: 1809-6514 ISSN Eletrônico: 2357-9501

SEGURANÇA DE REDES DE COMPUTADORES NA INTERNET

SECURITY OF COMPUTER NETWORKS ON INTERNET

Johnatan da Silva Costa
Bacharel em Administração/Faculdade Santo Agostinho
Teresina, Piauí, Brasil

Jovina da Silva
Mestre em Educação/Universidade Federal do Piauí
Teresina, Piauí, Brasil

Maria Auxiliadora Pereira da Cruz*
Mestra em Administração/Universidade Federal da Paraíba
Professora do Centro de Ensino Unificado de Teresina
E-mail: madoracruz@gmail.com
Teresina, Piauí, Brasil

*Endereço: Maria Auxiliadora Pereira da Cruz
Centro de Ensino Unificado de Teresina, Coordenação do Curso de Administração, Av. dos Expedicionários, 790 - São João, Teresina, PI - Brasil, CEP: 64046-700.

Editora-chefe: Dra. Marlene Araújo de Carvalho/Faculdade Santo Agostinho

Artigo recebido em 14/05/2012. Última versão recebida em 05/06/2012. Aprovado em 06/06/2012.

Avaliado pelo sistema Triple Review: a) Desk Review pelo Editor-Chefe; e b) Double BlindReview (avaliação cega por dois avaliadores da área).

RESUMO

Este estudo apresenta uma análise dos aspectos relativos aos cuidados com a segurança de redes de computadores, descrevendo da literatura, algumas das ameaças bem como elementos de segurança de redes. Portanto, centrou-se nas ameaças referentes à invasão, vírus, e roubo de informações , devido ao aumento da incidência de casos desse tipo. Também procurou-se mostrar mecanismos de previsões e tendências na área de segurança de computadores para um futuro próximo. Trata-se de um estudo teórico-metodológico, os resultados evidenciam que as empresas já estão se preparando para o enfrentamento dessa problemática e que há ainda um mercado aberto a ser explorado por profissionais da área. Por fim, apresenta-se considerações e sugestões sobre como se minimizar a insegurança em rede.

Palavras- chave: Segurança na internet. Vírus. Invasão. Rede de computadores.

ABSTRACT

This study presents an analysis of the aspects related to the security cares for computers net, describing from literature, some of the threats as well as elements of nets. Therefore, it was centered in the referring threats related to invasion, virus and robbery of information, due to the increase of these cases nowadays. It also looked for the opportunity to show preview mechanisms and trends in the computer security area for a near future. It brings a theoretical-methodological study that shows that the companies are getting ready to face this problematic and it represents an open market as a great opportunity for the professionals working in this area. Finally, it presents suggestions about how to minimize the risks and non-security in computer networks.

Keywords: Security in computer networks. Computer virus. Invasion. Computer networks.

1 INTRODUÇÃO

A princípio, o sistema de redes foi projetado com o objetivo de pesquisa, com a finalidade fundamental de estabelecer interatividade entre computadores, portanto, a segurança estava ausente no sistema. Ao longo dos anos as organizações perceberam a necessidade de implementar um sistema prático e viável a longo prazo. Na realidade atual, com o crescimento da demanda comercial cada vez mais acentuada, a segurança tornou-se necessária. Na administração organizacional, a informação é de grande importância como ativo permanente da empresa; deve ser considerada na estrutura do sistema de segurança e claramente estabelecida por uma classificação no controle de informações para que futuramente sejam acessadas, evitando a invasão por pessoas não autorizadas.

A operação do sistema em rede possibilita muitos benefícios, ganhos de produtividade em virtude do compartilhamento de recursos e propagação ou disseminação da informação, inclusive com o objetivo de divulgação. Porém, esses benefícios trazem alguns riscos como todo e qualquer sistema. Conectar-se em rede significa possibilitar condições específicas de controle com acesso externo aos recursos no contexto computacional, principalmente às informações. As falhas decorrentes da ausência de medidas de segurança para proteção permitem condições de controle e acesso que podem ser exploradas por usuários externos ou internos ao sistema de computação, obtendo acesso não autorizado. As falhas no sistema podem ser causadas por impactos de diferentes níveis havendo uma ambivalência, partindo desde uma simples ameaça, até uma ação que comprometa a imagem corporativa, chegando a perdas financeiras e de mercado a longo prazo.

Com o advento da implantação do sistema de redes, o crescimento da sua utilização, tornou-se fundamental para a armazenagem de informações. Dificilmente podemos imaginar os bancos sem o advento das redes de computadores. Transações são efetuadas simultaneamente, acesso a home banking, atendimento automático e outros recursos específicos na área.

Os sistemas de redes de computadores proporcionam processos mais dinâmicos, rápidos com menores custos e produtividade aumentada por colaboradores remotos e móveis. Estes se tornaram chave propulsora para que as organizações continuem competitivas. Neste sentido, o colaborador poderá acessar os dados corporativos remotamente e fechar o negócio com seu cliente de modo rápido e, consequentemente minimizando tempo e custos, ganhando vantagem em relação a quem precisa enviar um memorando à centralizadora para confirmar se existe disponibilidade do produto negociado.

A Segurança de redes é um requisito extremamente divulgado na mídia em geral. Atualmente, apesar dos problemas constantes e perigos referentes à segurança das redes de computadores, a maioria das empresas não possuem estrutura necessária para enfrentar os problemas freqüentes no uso de rede.

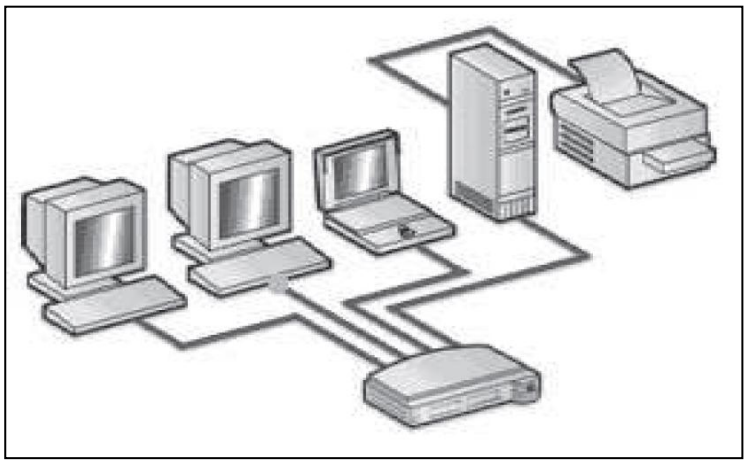
Nesse trabalho, descrevem-se alguns dos problemas e ameaças relativos à segurança de redes de computadores, especificamente sobre invasões de redes e perdas financeiras causadas por vírus de computador. A opção pelo estudo deve-se ao fato de perceber - se um aumento negativo na incidência desses tipos de problemas em relação ao sistema.

Enfatizou-se uma descrição de recursos como ferramentas e métodos utilizados para a proteção e segurança de redes de computadores. Não é finalidade deste artigo apresentar um guia completo para a implantação de métodos de segurança de redes. Cada ferramenta ou problema no sistema de rede é complexo o bastante para ser objeto de um estudo.

2 REDE DE COMPUTADORES

No ambiente do sistema de rede de computadores, procura-se mostrar as definições dos temas que serão apresentados nos tópicos subseqüentes: Redes de computadores, seus objetivos, o aumento constante do seu uso e os princípios básicos que norteiam a segurança de redes de computadores. A figura abaixo representa um exemplo do fluxograma de rede de computadores.

Figura1 – Fluxograma de rede de computadores.



Fonte: http://www.timaster.com.br

2.1 Rede de Computadores

As redes de computadores abrangem qualquer sistema interconectado através de núcleos de processamento. Permite o usuário acessar remotamente um terminal de outro computador situado no sistema. A rede local é um sistema de comunicação que possibilita a interatividade de uma variedade de mecanismos. A seguir três aspectos básicos para compreensão:

- Rede local é uma rede de comunicação de dados;
- É elaborada e estabelecida para interconectar uma grande variedade de dispositivos, de diferentes tipos;
- Tem uma abrangência geográfica restrita sem relação aos similares de comunicação de dados existentes, tais como a rede de longo alcance ou uma rede de teleprocessamento. De acordo com Pinheiro (2005, p. 1):

> Independente do tamanho e do grau de complexidade, o objetivo básico de uma rede de computadores é garantir que todos os recursos de informação sejam compartilhados rapidamente, com segurança e de forma confiável. Para tanto, a rede deve possuir meios de transmissão eficientes, regras básicas (protocolos) e mecanismos capazes de garantir o transporte das informações entre os seus elementos constituintes.

A operacionalização de uma rede de computadores tem como objetivos básicos prover a comunicação confiável entre os vários sistemas de informação, melhorar o fluxo e o acesso às informações, bem como agilizar a tomada de decisões administrativas facilitando a comunicação entre seus usuários.

2.2 Objetivos das redes de computadores

Tanebaum (1994) define os objetivos das interconexões de computadores autônomos como sendo:

- **Compartilhamento de recursos:** Fazer com que todos os programas, dados e equipamentos da rede estejam disponíveis a todos os usuários independentemente de sua localização física. Como exemplo, pode citar-se o compartilhamento de uma impressora por vários usuários;
- **Economia:** A substituição gradativa dos antigos mainframes para as redes de computadores de pequeno pote, significou uma redução muito grande nos custos de

manutenção dos sistemas de informação possibilitando uma verdadeira revolução nos CPDS. Esse fenômeno ficou conhecido mundialmente como Downsizing. Essas redes de computadores de pequeno porte possibilitam um aumento da capacidade de processamento a medida que a demanda cresce , ao contrário dos grandes mainframes, onde a sobrecarga só poderia ser solucionada com a substituição do mesmo por um mainframe de maior capacidade , a um custo geralmente muito elevado.

- **Prover um meio de comunicação:** As redes de computadores também são um poderoso meio de comunicação entre pessoas, possibilitando inclusive o trabalho em conjunto, mesmo estando a quilômetros de distância.

2.3 Crescimento do uso das redes de computadores

Com o advento da globalização a partir do século XX, a demanda tornou-se extremamente capitalista, surgindo novas necessidades de conquistar qualidade e eficiência no serviço a custo baixo. A grande quantidade de dados ou informações a serem processadas e armazenas demonstram um volume incalculável. O sistema de redes surge neste contexto: para superar a necessidade do ser humano de controlar os dados em abundância com precisão e rapidez.

O crescimento freqüente e notável do sistema de redes e a disponibilização de recursos vêm possibilitando comunicação com maior eficiência. As redes contribuem significativamente para uma modificação na comunicação atual. Os colaboradores ou usuários se intercomunicam, trocam informações a fim de minimizar o tempo e custos.

2.4 Princípios Básicos da Segurança de Redes de Computadores

A *San Francisco State University* (1991) define o propósito da Segurança de Computadores como sendo "a proteção do local onde está o computador, seu hardware, software e dados nele armazenados". Essa responsabilidade é compartilhada por todos os usuários que utilizem a rede de computadores.

A perfeita segurança no sistema de rede é utopia, portanto devemos prevenir ou reduzir a probabilidade de danos ao hardware, software e aos dados. Os danos podem ser provenientes de:

- Mau uso (acidental ou proposital);
- Dano por vandalismo;

- Invasão intencional;
- Fraude;
- Sabotagem;
- Desastres por fogo, água, terremotos, furações, etc.

Cox (2001) Enfatiza três aspectos básicos para segurança de dados que se subdividem em vários tópicos:

a) Prevenção – Consiste em se evitar que aconteçam os problemas. Compreende os seguintes procedimentos:

Proteção de hardware: normalmente chamado de segurança física, é de vital importância. Negando acessos físicos não autorizados a infra- estrutura da rede, previne-se de possíveis roubos de dados, desligamento de equipamentos e demais possíveis quando se esta fisicamente no local;

Proteção de arquivos e dados: providenciando por autenticação, controle de acesso e antivírus. No processo de autenticação, é verificado se quem está pedindo acesso é realmente quem diz ser. No processo de controle de acesso, só são disponibilizadas as transações realmente pertinentes a essa pessoa (ex.: só leitura de arquivos, leitura e escrita, quais pastas ou arquivos a pessoa pode utilizar, etc.);

Proteção do perímetro da rede: ferramentas firewall cuidam desse aspecto, mantendo a rede protegida contra invasões de usuários não autorizados.

b) Detecção – Refere-se ao fato de detectar o problema o mais cedo possível, através de:

Alertas: sistemas de detecção de intrusos (IDS- *Intrusion Detection System- Sistemas de Detecção de Intrusos*- Item 2.3.5) podem avisar os administradores e responsáveis pela segurança da rede a qualquer sinal de invasão ou mudança suspeita no comportamento da rede que pareça um padrão de ataque ou mude o comportamento normal da rede. Os avisos podem ser via e-mail, via mensagem no terminal do administrador, e outros;

Auditoria: periodicamente deve-se analisar os componentes críticos do sistema à procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho nos arquivos de senhas, usuários com inatividade longa, etc.

c) Recuperação – Retomar o funcionamento normal após o incidente. Adotando as seguintes medidas básicas:

Cópia de segurança dos dados (Backup): manter completo, atualizado e testado, backup dos dados em meio diferente e separado dos servidores;

Aplicação para realizar o Backup: ferramentas que proporcionem recuperação rápida dos dados do backup;

Backup do Hardware: a compra ou utilização de backup de hardware (ex: servidor reserva, no-break reserva, linhas de dados reserva, etc.) podem ser justificados, levando-se em conta o custo de uma parada do sistema e determinando-se a importância da informática para a organização.

Vulnerabilidades: pontos suscetíveis a ataques, causados por uma brecha do software ou hardware, má configuração e administração ou ambos.

Ameaças: problemas que podem atacar as vulnerabilidades. Normalmente são agrupadas em três categorias: pessoais (ex.: omissão ou intenção criminal), de peças (ex.: falha de um equipamento) ou de eventos (ex.: fogo, inundação);

Proteções: técnicas para proteger-se contra uma ameaça.

No contexto do sistema mundial relacionado à rede de segurança de computadores, define-se três princípios gerais básicos para mantê-lo de forma eficiente:

Confidencialidade: proteger contra a revelação acidental ou deliberada de informações críticas;

Integridade: proteger contra corrupção deliberada ou acidental de informações;

Disponilidade: proteger contra ações que causem a indisponibilidade de informações críticas aos usuários quando necessitarem.

2.5 Ameaças e Problemas de Segurança de Redes de Computadores

Nesse enfoque, descrevem-se algumas das ameaças a Segurança de Redes de Computadores.

2.5.1 *HACKERS*

O hacker é um indivíduo que objetiva explorar minuciosamente os sistemas e descobrir como obter o máximo de sua capacidade, em oposição à maioria dos usuários

convencionais, que preferem aprender apenas o necessário para satisfazer suas necessidades básicas. Outra definição: aquele que programa de forma obsessiva sem limites, ou seja, o indivíduo insaciável que prima pela tecnologia de informação (ti); o *hacker* que se dedica a roubar arquivos ou destruir dados ganha outro nome: *cracker*. Esses são os hackers perigosos, os verdadeiros criminosos virtuais; são indivíduos que quebram a segurança do sistema ou ganham acesso a sistemas de outras pessoas involuntariamente.

***Sninffing* ou "farejar"**: procura de senhas de acesso. Mcclure, Scambray e Kurtz (2000,p.61), definem:

> os sniffers ou farejadores com ferramentas incialmente projetadas para verificar problemas em redes de computadores, que tiveram seu uso deturpado pelos crackers". coleta e armazena pacotes que está em transações constantes pela rede para a análise posterior. Os crackers utilizam os dados ou informações coletados para pesquisa de senhas e nomes de usuários.

***Password cracking* ou "quebra de senha"**: atividade em que o *cracker* tenta descobrir as senhas de acesso de um usuário capturado pelo processo de *sniffing*, por exemplo, quando a senha está criptografada. Caso não esteja, esse passo não é importante. A maneira mais convencional é o de tentativas, conhecido como *Brute-Force Atac*k, uma técnica de criptoanálise onde se tentam diversas possibilidades possíveis, minuciosamente. Nesse ataque, o invasor utiliza programas como dicionários de palavras conhecidas e suas combinações. Com o desempenho atual dos computadores um programa dessa natureza tem condições de efetuar milhares de tentativas para descriptografar a senha a curto prazo.

***Spoofing* ou "fingimento":** Ataque no qual o intruso finge ser um computador conhecido do alvo do ataque para ultrapassar ou invadir suas defesas. Cross (2002, p.32), "explica que esse tipo de ataque é feito com ferramentas que trocam os cabeçalhos IP da comunicação, fazendo com que a vítima pense estar se comunicando com um computador confiável".

2.5.2 VÍRUS

O vírus é uma parte de *software* ou programa de computador projetado com a finalidade de se auto replicar e se disseminar em várias partes do sistema. Atualmente, os chamados vírus de computador são classificados em vários tipos, cada um com suas peculiaridades de funcionamento e contágio.

Alguns vírus se manifestam causando danos a arquivos do sistema que estejam infectando. Mas não necessariamente ele causa danos ao sistema, eles são essenciais na definição de um vírus. Um vírus inócuo (que não causa danos) continua sendo um vírus.

Não existem vírus simplesmente porque o código do vírus não foi instalado intencionalmente pelo usuário. Os usuários finais têm livre arbítrio para manter o controle sobre seus computadores e isto inclui a liberdade de instalar e remover software: nenhum software pode ser instalado, modificado ou removido sem o conhecimento e a permissão do usuário. Um vírus é auto-instalado, pode modificar toda a estrutura do sistema envolvido, corrompendo as informações.

Dentre eles, os principais tipos são:

Vírus de *boot*: fixam-se em num setor onde se encontra o código que o micro computador executa automaticamente quando é ligado (*boot* frio) ou é "resetado" (*boot* quente). Dessa forma, os vírus são carregados e executados toda vez que ocorrer um boot. Após as informações serem carregadas, eles carregam o código de boot original do micro, o qual foi deslocado pelo vírus para outra parte do sistema.

Vírus simples: a RFC 2828 (Request for Coments nº 2828) define um vírus de computador como sendo um software com capacidade de se duplicar, infectando outros programas, usualmente com alguma intenção maliciosa. Um vírus não pode executar-se sozinho, requer que o seu programa hospedeiro seja executado para ativar o vírus;

Cavalos de tróia: é definido pela mesma RFC. É um programa que aparenta ter uma função útil, mas possui alguma função maliciosa que interfere nos os mecanismos de segurança. Não possui a capacidade de se replicar.

***Worm* ou "verme"**: definido pela mesma RFC como sendo um programa de computador que pode se executar independentemente, propagar-se pelos computadores de uma rede independente, podendo consumir os recursos dos computadores destrutivamente;

Vírus polimorfo: tipo de vírus que modifica a si mesmo a medida que se dissemina, dificultando a sua localização e eliminação;

Vírus de Macro: utiliza-se da linguagem VBScript dos software Microsoft e pode ser executado em qualquer computador que possua, por exemplo, o aplicativo Word instalado.

3 CONSIDERAÇÕES FINAIS

A segurança em redes de computadores é uma questão complexa. Esse é uma desafio a ser enfrentado pelas organizações que visam obter lucro, minimizar tempo e reduzir os custos,

portanto é uma ferramenta importante inerente à infra- estrutura. Os procedimentos e recursos de segurança devem ser vistos como prioridade e consequentemente em constante reavaliação dentro das corporações. Neste cenário simultaneamente amigável e hostil que o sistema de rede de segurança oferece, exige-se profissional capaz de perceber as limitações e tomar as decisões adequadas para resolvê-las. Considerando esse pressuposto, devesse levar em consideração os seguintes aspectos:

- A estratégia de segurança adotada está de acordo com as necessidades da organização?
- O *staff* da organização recebe atenção devida no que diz respeito à segurança das informações que armazenam em seus computadores? A cultura de segurança está disseminada entre eles?
- Estrutura, funcionalidade e orçamento dedicados a segurança estão compatíveis com a estratégia de negócios da organização? Existe medição sobre o retorno dos investimentos com segurança?
- Qual a abrangência e profundidade com que se trata a segurança nos ativos eletrônicos da corporação? Tomam-se medidas que vão além da implantação de ferramentas e produtos para proteção?
- Qual o impacto que as falhas de segurança podem provocar na relação de confiança e fidelização com os clientes, parceiros e colaboradores?

O objetivo de reavaliar segurança nas organizações, imposta pela nova realidade global, não deve tirar o foco de negócios. Por outro lado, não é desejável que se tomem decisões a partir de análises superficiais ou de direcionamentos extremistas e pouco flexíveis, fundamentados simplesmente por medo e insegurança.

Estabelecer medidas de segurança é sem dúvida um trabalho cauteloso e a longo prazo exatamente o oposto do tipo de trabalho que a maioria dos técnicos realizam. Isso é vital para a segurança da instituição.

Manter *firewalls* de forma eficaz e em concordância com medidas de segurança é também um trabalho de excelência. O conjunto de sistemas computacionais que filtra conteúdo deve ser um espelho daquilo que a diretoria da corporação espera do cumprimento da política de uso da Internet, bem como deve minimizar as possibilidades de ataques, invasões e vazamento de informação, mantendo a integridade e reputação da instituição.

Acredita-se que o modelo de proteção apresentando neste trabalho é de grande utilidade quando se visa custo/beneficio, maximização de lucros e minimização de tempo a

longo prazo. Portanto, indica-se esse estudo a todos os interessados no assunto que desejam garantir um espaço no mercado atual.

REFERÊNCIAS

COX, W. **The Critical security issue**. 2001. Disponível em: <www.sans.org>. Acessado em: 24 abr. 2010.

CROSS, S. E. **Cyber threats and the U.S.** Economy, 2000. Disponível em: <www.cert.org>. Acessado em: 05 ago. 2010.

SANTOS, P. **Sistemas estruturados em redes de computadores**. Disponível em: <http://www.projetoderedes.com.br>. Acessado em: 02 jun. 2011.

TANENBAUM, A. S. **Redes de computadores.** Rio de Janeiro: Campos, 1994.