

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

ESTADO DA ARTE EM SEGURANÇA DE SISTEMAS VIA INTERNET

ESTADO DA ARTE EM SEGURANÇA DE SISTEMAS VIA INTERNET

Monografia apresentada ao
Curso de Graduação em
Sistemas de Informação da
Faculdade Natalense para o
Desenvolvimento do Rio Grande do
Norte como requisito parcial para
obtenção do grau de Bacharel
em Sistemas de Informação

Orientador:

Mounarte Leitão de Medeiros Brito

Felipe Araújo Almeida, MSc.

NATAL

2002

LIGA DE ENSINO DO RIO GRANDE DO NORTE
MOUNARTE LEITÃO DE MEDEIROS BRITO
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ESTADO DA ARTE EM SEGURANÇA DE SISTEMAS VIA INTERNET



Mounarte Leitão de Medeiros Brito

Monografia apresentada ao
Curso de Graduação em
Sistemas de Informação da
Faculdade Natalense para o
Desenvolvimento do Rio Grande do
Norte como requisito parcial para
obtenção do grau de Bacharel
em Sistemas de Informação

Orientador:

Fellipe Araújo Aleixo, MsC.

NATAL
2002



004.7.004.4
B877e
2002

Brito, Mounarte Leitão de Medeiros

Estado da Arte em Segurança de Sistemas Via Internet/Mounarte Leitão de Medeiros
Brito. Natal: FARN, 2002.

84p.

Monografia (Bacharelado em Sistemas de Informação) – Faculdade Natalense para o
Desenvolvimento do Rio Grande do Norte.

1. Informática – Monografia 2. Segurança de redes I. Título

RN/FARN/BC

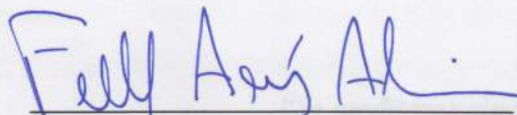
CDU 004.7

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

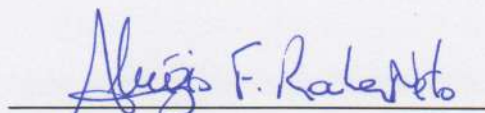
ESTADO DA ARTE EM SEGURANÇA DE SISTEMAS VIA INTERNET

Mounarte Leitão de Medeiros Brito

Monografia apresentada e aprovada em 14 de DEZEMBRO de 2002.
pela banca examinadora composta pelos seguintes membros.



Prof. Felipe Araújo Aleixo, MsC.
Orientador


Profa. Livia Maria Martins da Silva

Prof. Aluizio Ferreira Rocha Neto

Natal, _____ de _____ de _____.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado a oportunidade de estar aqui e a Virgem Maria por me dar forças para que eu nunca desistisse.

A Minha Esposa Ellen, que me incentivava a abraçar com garra e determinação cada oportunidade que a vida me ofereça.

As minhas filhas, Mariana e Fernanda, e a Leonardo da Vinci, que sabem me fazer feliz como ninguém.

Agradeço à minha mãe Nininha, ao meu pai Genarte e a minha sogra Graça Mota, vocês sempre me apoiaram em minhas decisões, sempre me incentivando e aconselhando nos momentos felizes e difíceis da vida.

Agradeço a meus irmãos Genarte Jr., Ricardo, Linduarte e Leonarte, companheiros de jornada e de lar.

Agradeço à minha cunhada Daniele e ao meu cunhado José Batista, irmãos espirituais, e em especial à minha cunhada Luciana Mota, que preso como uma grande amiga e grande companheira de luta.

Agradeço a todos meus familiares e amigos.

Agradeço à Am. Angelica, Daniele Lobo, Jackson Almeida, Vanessa, Sebastião Clemente e Rodrigo Bruno, amigos que fiz durante o curso e espero que continuem sendo meus amigos...

A minha coordenadora Livia Maria por

Ao professor e orientador Felipe Araújo, que me aplicou, me orientou e me deu liberdade para me interessar. Sua paciência e apoio foram muito importantes, principalmente na reta final do meu trabalho.

"Se meditares sinceramente na provas que já venceste, nos problemas que já atravessaste, nas dores que já esqueceste e nos obstáculos que, muitas vezes, já contornaste, reconhecerás que o amparo de Deus esteve e está contigo em todos os momentos!"

Emmanuel

Agradeço a família FARN, todos os meus professores durante o curso, funcionários, direção e alunos que me acolheram e ajudaram no meu aprendizado.

Agradeço àqueles que me ensinaram, que sorriram, que festejaram, que conversaram, que confidenciaram, que choraram, que discutiram, que escutaram, que assistiram, que cobraram, que conviveram e que de alguma forma, mesmo que por alguns instantes, fizeram parte da minha história durante o tempo em que estive nesta Faculdade.

E todos que, de alguma forma, contribuíram na elaboração deste trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado a oportunidade de estar aqui e a Virgem Maria por me dar forças para que eu nunca desistisse.

À Minha Esposa Ellen, que me incentiva a abraçar com garra e determinação cada oportunidade que a vida me oferece.

As minhas filhas, Mariana e Fernanda, e a Leonardo da Vinci, que sabem me fazer feliz como ninguém.

Agradeço à minha mãe Nininha, ao meu pai Genarte e a minha sogra Graça Motta, vocês sempre me apoiaram em minhas decisões, sempre me incentivando e aconselhando nos momentos felizes e difíceis da vida.

Agradeço a meus irmãos Genarte Jr., Ricarte, Linduarte e Leonarte, companheiros de jornada e de lar.

Agradeço a minha cunhada Daniele e ao meu cunhado José Batista, irmãos espirituais, e em especial à minha cunhada Luciana Mota, que preso como uma grande amiga e grande companheira de luta.

Agradeço a todos meus familiares e amigos.

Agradeço à Ana Angélica, Daniele Lobo, Jailson Almeida, Vanessa, Sebastião Clemente e Rodrigo Bruno, amigos que fiz durante o curso e espero que continuem sendo meus amigos...

A minha coordenadora Lívia Maria por tudo que fez por mim e por nossa turma.

Ao professor e orientador Felliipe Araújo Aleixo que, mesmo eu sendo um aluno não tão aplicado, me orientou e me deu liberdade para trabalhar no projeto que mais me interessou. Sua paciência e apoio foram muito importantes, principalmente na reta final do meu trabalho.

Agradeço a família FARN, todos os meus professores durante o curso, funcionários, direção e alunos que me acolheram e ajudaram no meu aprendizado.

Agradeço àqueles que me ensinaram, que sorriram, que festejaram, que conversaram, que confidenciaram, que choraram, que discutiram, que escutaram, que assistiram, que cobraram, que conviveram e que de alguma forma, mesmo que por alguns instantes, fizeram parte da minha história durante o tempo em que estive nesta Faculdade.

E todos que, de alguma forma, contribuíram na elaboração deste trabalho.

SUMÁRIO

1.2.2	spoofing ou "fingir"	40
1.2.3	Ataques de negação de serviço	40
1.2.3.1	Falhas de protocolo	41
1.	Introdução	12
1.1	Apresentação	12
1.2	O problema	15
1.3	Objetivo	16
1.4	Metodologia	16
1.5	Estrutura	17
2.	Referencial Teórico	18
2.1	Redes de computadores	18
2.1.1	Objetivos das redes de computadores	20
2.1.2	Conjunto de protocolos tcp/ip	20
2.1.3	Internet	22
2.2	Os Sistemas distribuídos	23
2.2.1	Aspectos de tolerância a falhas	24
2.2.2	Vantagens e desvantagens	25
2.2.2.1	Vantagens do sistema distribuído sobre os centralizados	24
2.2.2.2	Vantagens do sistema distribuído sobre pcs independentes	25
2.2.2.3	Desvantagens dos sistemas distribuídos	25
2.3	Segurança em redes de computadores	26
2.3.1	Política de segurança	28
2.3.2	Tipos de segurança de dados	30
2.3.3	Propriedades de segurança	32
2.3.4	Vulnerabilidades de segurança de sistemas baseados em redes	32
3.	Problemas e soluções para segurança de redes de computadores	35
3.1	Considerações Iniciais	35
3.1.1	Objetivos da resposta a incidentes de segurança	35
3.1.2	Metodologia de resposta a incidentes de segurança	36
3.1.3	Métodos de ataque	38
3.2	Mecanismos de ataque	40
3.2.1	Sniffing ou "farejar"	40

3.2.2	Spoofing ou “fingimento”	40
3.2.3	Ataques de negação de serviço	40
3.2.3.1	Falhas de protocolo	41
3.2.3.2	<i>Smurf</i>	41
3.2.3.3	Interrupção de serviço	41
3.2.3.4	<i>Denial of service</i> (dos)	41
3.2.3.5	Ping of death (ping da morte), flooding (inundação), smurfing, denial of service (negação de serviço)	42
3.2.4	Vírus	42
3.2.4.1	Vírus simples	43
3.2.4.2	Cavalos de tróia ou <i>trojan</i>	43
3.2.4.3	<i>Worm</i> ou “verme”	43
3.2.4.4	Vírus polimorfo	43
3.2.4.5	Vírus de macro	43
3.2.4.6	Vírus de disco	43
3.2.4.7	Vírus companheiros	44
3.2.5	<i>Back door</i> - porta dos fundos	44
3.2.6	Cracker de senha - <i>password cracking</i>	45
3.3	Mecanismos de defesa	45
3.4.1	Criptografia	46
3.4.2	Kerberos	48
3.4.3	<i>Firewall</i>	48
3.4.4	IDS – <i>Intrusion detection system</i>	50
3.4.5	Senhas e autenticação	50
3.4.6	Antivírus	50
3.4.7	Alertas	50
3.4.8	Tabela resumo de ataques e contramedidas – defesa	52
4.	Conclusão	57
5.	Glossário	58
	Referências bibliográficas	82
	Bibliografia	83

LISTA DE ILUSTRAÇÕES

Figura 1. Microcomputador padrão PC.....	12
Figura 2. Redes de Computadores.....	13
Figura 3. Gráfico de empresas Brasileiras que possui política de segurança.....	29
Figura 4. Gráfico dos tópicos abordados na política de segurança.....	30
Figura 5. Diagrama de resposta a incidentes de segurança.....	37
Figura 6. Gráfico das principais ameaças a segurança de Sistemas Distribuídos.....	38
Figura 7. Gráfico dos principais responsáveis por problemas com segurança.....	39
Figura 8. Gráfico da contaminação por vírus em Empresas Brasileiras	42
Figura 9. Gráfico das principais medidas de segurança adotadas.....	45
Figura 10. Modelo de <i>Firewall</i>	49

LAN - Local Area Network

MAC - Media Access Control

IPSG - Packet InterNet Group

POP - Post Office Protocol

REC - Request For Comments

RIP - Routing Information Protocol

SMTP - Simple Mail Transfer Protocol

SNMP - Simple Network Management Protocol

STP - Shielded Twisted Pair

TCP - Transmission Control Protocol

LISTA DE ABREVIACÕES

ARP - Address Resolution Protocol

CERT - Computer Emergency Response Team

CRC - Cyclic Redundancy Check

DNS - Domain Name Service

DoS - Denial of Service

FTP - File Transfer Protocol

ICMP - Internet Control Message Protocol

IP - Internet Protocol

LAN - Local Area Network

MAC - Media Access Control

PING - Packet InterNet Groper

POP - Post Office Protocol

RFC - Request For Comments

RIP - Routing Information Protocol

SMTP - Simple Mail Transfer Protocol

SNMP - Simple Network Management Protocol

STP - Shielded Twisted Pair

TCP - Transmission Control Protocol

RESUMO

Neste trabalho, organizado na forma de monografia, procurou-se demonstrar os principais aspectos relativos à Segurança de Redes de Computadores, descrevendo na revisão da literatura, algumas das ameaças e alguns elementos de Segurança de Redes de Computadores.

Em primeira instância, são apresentados alguns conceitos básicos sobre Segurança: Integridade dos Dados, Confidencialidade, Identificação, Autenticação, Autorização e Controle de Acessos.

Em seguida, são descritas as características dos seguintes métodos de ataque: Vírus, Cavalo de Tróia, Trap Doors, Spoofing e Sniffing. Para garantir a privacidade dos dados de forma que somente as máquinas envolvidas na comunicação tenham acesso a elas, faz-se uso de algoritmos de criptografia. Técnicas mais modernas como o uso de Firewall podem resolver problemas de falsificação de endereços e evitar a entrada de mensagens maliciosas.

1 - INTRODUÇÃO

1.1 - APRESENTAÇÃO

ABSTRACT

In this work, organized as a Monography, we are try to demonstrate the most important aspects of Computer Network Security, describing at the literature review, some of the threats and elements of the Computer Network Security.

In a first sight, there are some basic concepts presented about Security: Data Integrity, Confidentiality, Identification, Authentication, Authorization, and Access Control .

Following, some characteristics are described about the attack methods: Viruses, Trojan Horses, Trap Doors, Spoofing e Sniffing.

To achieve data's privacy, its necessary to user cryptography algorithms. More modern techniques, like Firewalls, solve problems of forged address and could stop dangerous messages.

1 – INTRODUÇÃO

1.1 – APRESENTAÇÃO

O computador moderno nasce das idéias sobre algoritmos, publicadas em 1937 por Alan Turing, e dos planos de John von Neumann para uma nova máquina de calcular que pela primeira vez inclui, além de cálculos matemáticos, o processamento lógico de informações. O primeiro computador operacional foi construído por Alan Turing e sua equipe para o serviço de inteligência britânico em 1940.

De 1945 a 1950: durante este período, foram fabricados os primeiros computadores, enquanto que, simultaneamente, eram construídas as últimas das grandes calculadoras. A partir do início da década de 50, o computador passa a ser comercializado em grande escala. Essa década é marcada pelo surgimento dos primeiros computadores civis e pelo desenvolvimento de grandes computadores militares.

Com a popularização do uso de computadores, as empresas visam melhorar o nível de produtividade, para isto aderiram às soluções de serviços baseados em redes de computadores, ou simplesmente, serviços em rede.

Os serviços em rede envolvem toda a infra-estrutura necessária para produtos (hardware e software) necessários para permitir que aplicações distribuídas sejam construídas e possam ser executadas de maneira consistente em um ambiente de rede distribuída (JÚNIOR, MOURA e TEIXEIRA, 1999).

As redes de computadores proporcionam, entre outros benefícios, processos mais rápidos, comunicações dinâmicas, produtividade aumentada por funcionários remotos e móveis, etc.

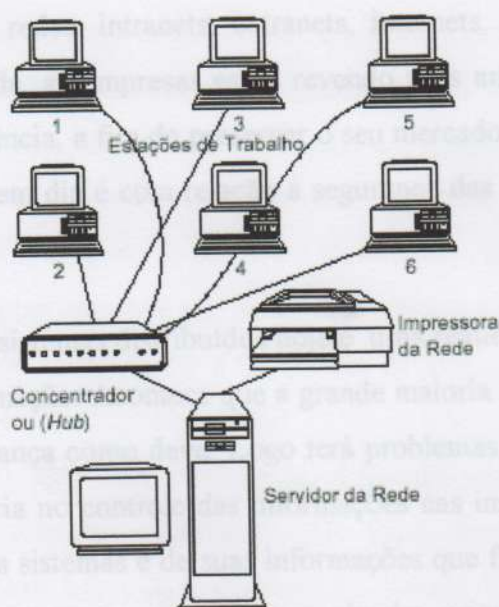


Figura 2 – Redes de Computadores

O avanço tecnológico possibilitou a criação da ARPANET, rede originada e patrocinada pela DARPA para interligar universidades e centros de pesquisa do Governo norte-americano. Esta foi a primeira a utilizar a pilha TCP/IP e que deu origem à internet. A ARPANET começou com aproximadamente 500 minicomputadores, cresceu até o início dos anos oitenta na velocidade de um servidor a cada três semanas. Hoje a Internet tem mais de 100.000.000 de usuários, e continua crescendo vertiginosamente.

A Internet não foi criada para ser utilizada por um número muito grande de pessoas, como acontece hoje. Por isso, às máquinas que a compõem têm sofrido constantemente vários ataques, muitos deles prejudiciais. Mesmo assim, o número de usuários tem crescido muito, mas as preocupações com segurança não. Ao passo que os usuários estão constantemente crescendo em números, as preocupações com segurança não crescem na mesma escala.

Esta rede privada era destinada a interligar os computadores dos centros de pesquisa, universidades e instituições militares americanas, permitindo o compartilhamento de recursos entre os pesquisadores que trabalhavam com projetos estratégico-militares.

A Internet evoluiu muito e foram criados novos serviços como *E-mail*, *World Wide Web*, *Gopher*, trânsito de informações sigilosas e o surgimento do comércio eletrônico ou mercado virtual que vem difundindo-se em todo o mundo há muito tempo, mas que atualmente está tomando espaço em áreas mais populares e acessíveis. Milhões de computadores se juntaram a ela e seus recursos são cada vez mais sofisticados.

Com a popularização das redes, intranets, extranets, internets, a globalização e a concorrência cada vez mais acirrada, as empresas estão revendo seus antigos paradigmas e buscando mecanismos de sobrevivência, a fim de preservar o seu mercado. Uma das grandes preocupações dos executivos hoje em dia é com relação à segurança das informações de sua empresa.

A insegurança em redes ou sistemas distribuídos hoje é uma realidade que preocupa o profissional de tecnologia da informação. Acontece que a grande maioria dos administradores hoje não se preocupa com a segurança como deve. Logo terá problemas com o seu sistema, não importa qual seja. A deficiência no controle das informações nas instituições tem como consequência a vulnerabilidade dos sistemas e de suas informações que ficam ameaçadas por ataques maliciosos, pois ao mesmo tempo em que tem alguém criando dificuldades ou implementando proteção, outras tantas pessoas estão estudando como burlar ou quebrar o modelo de segurança através do uso de ferramentas ou mecanismos do tipo: vírus, cavalo de tróia.

A história da segurança na informática começou em torno dos anos 50, nessa época a informática estava ainda engatinhando e pouca coisa se sabia sobre proteção. Somente a partir de 1984, depois que os ataques a computadores começaram a se multiplicar e proporcionar grandes prejuízos, é que nos Estados Unidos foi implantado os procedimentos para garantir a invulnerabilidade dos computadores. Atualmente, a consciência sobre segurança em informática no Brasil começa a evoluir, nossas empresas, instituições e usuários se planejam para garantir a confiabilidade de suas informações (dados).

O primeiro conceito relacionado a segurança é: "não existe sistema completamente seguro", este fato obriga todo e qualquer administrador a preocupar-se com a segurança de seus sistemas. A segurança das redes e da informação pode ser entendida como a capacidade de uma rede ou sistema da informação para resistir, com um dado nível de confiança, a eventos acidentais ou ações maliciosas. Estes eventos ou ações podem comprometer a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos através dessa rede ou sistema. Na atualidade, a informação é tratada como ativo da empresa, a informação pode estar impressa, manuscrita, gravada em meios magnéticos, ou simplesmente, ser do conhecimento dos funcionários.

A finalidade de toda análise de segurança consiste em fundamentar a especificação de como os níveis de segurança desejados devem ser atingidos. Assim, depois de conhecer a ameaça, deve-se projetar mecanismos para prevenir, detectar ou recuperar-se de um ataque. Nesse sentido, são desenvolvidas diversas ferramentas para avaliação das vulnerabilidades das redes, bem como para sua proteção, onde se destacam técnicas de criptografia e softwares firewalls e proxies. Essas ferramentas possibilitam, além da proteção preventiva do sistema, a realização de auditorias que permitam identificar a ocorrência de ataques e rastrear a origem destes.

Ao passo que as empresas forem amadurecendo, a função segurança vai galgando camadas mais altas até alcançar o estratégico da organização. Desta forma conseguir emanar ações preventivas e pró-ativas durante a fase de elaboração dos planos. Para usar uma máxima do momento: "é pensar globalmente e agir localmente".

1.2 O PROBLEMA

É indiscutível os benefícios trazidos para a sociedade pelo aumento da tecnologia, pelo uso de computadores, e pelo avanço das comunicações mundiais, em especial da Rede Internacional de Dados - Internet, fomentando, sem precedentes na história, a paixão humana pelo conhecimento, educação e cultura.

Entretanto, esses benefícios não aparecem sozinhos, trazem consigo os crimes e criminosos digitais, os quais estão aumentando proporcionalmente por todo o mundo, sendo que as mais otimistas previsões apontam para um epidêmico e exponencial crescimento.

O uso de Internet / Intranet exige ainda segurança nos servidores. Recentemente, um hacker invadiu um servidor Internet de comércio eletrônico e roubou 100.000 números de cartões de crédito. Foi preso pelo FBI quando tentava vendê-los por US\$ 260.000 em dinheiro.

1.4 METODOLOGIA

Além do roubo de informações, uso e acesso indevido, outro problema sério para a segurança dos servidores nas empresas é a "pichação de sites", situação em que o site corporativo da empresa é invadido pela Internet e tem seus arquivos alterados para imagens

pornográficas ou dados falsos, acarretando sérios problemas na imagem ou reputação da empresa.

1.3 OBJETIVO

Apesar dos problemas, podemos afirmar que o uso adequado da tecnologia de segurança e dos mecanismos de proteção e controle na Internet e Intranet permitem realizar operações comerciais em condições mais seguras do que os meios de transações e comunicações convencionais. Por isso procuramos conscientizar de que é necessário que se implante uma Política de Segurança Corporativa com definição clara das diretrizes, normas, padrões e procedimentos que devem ser seguidos por todos os usuários;

Os negócios e novos mercados estão se direcionando cada vez mais para a Internet e Intranets. Torna-se necessário o conhecimento e análise dos riscos e vulnerabilidades a que estamos expostos, de forma que possamos definir os mecanismos adequados para a segurança.

A presente monografia tem por objetivo discorrer sobre o tema da segurança em Sistemas distribuídos, delimitando assuntos que figuram com grande frequência no cenário mundial através dos meios de comunicação de massa, demonstrando a fragilidade dos sistemas utilizados pelas empresas ou instituições, diante de invasões externas. As tecnologias direcionadas a segurança na área de tecnologia de informação é certamente uma área em crescimento. Diversas tecnologias surgem. Mas o que faz da escolha de um sistema de segurança uma coisa tão complexa? Que mecanismo de defesa escolher para deixar meu sistema seguro? As respostas a estas questões serão discutidas ao longo deste trabalho onde apresentaremos mecanismos de ataques mais comuns utilizados em sistemas distribuídos e os mecanismos de defesas utilizados para proteger os sistemas distribuídos dessas ameaças com o intuito de contribuir para que a sua escolha seja a melhor e mais prática para proporcionar a sua segurança.

1.4 METODOLOGIA

Para realização desse trabalho foi feita uma pesquisa bibliográfica e a análise de casos de quebra de segurança em sistema de redes descritos na literatura.

1.5 ESTRUTURA

Esta monografia foi dividida em três capítulos além da Introdução, descritos a seguir.

O Segundo Capítulo apresenta os fundamentos teóricos de sistemas distribuídos. O capítulo segue com ênfase em política de segurança e modelo de segurança.

O Terceiro Capítulo apresenta os métodos e os mecanismos de ataque e os métodos e mecanismos de defesa.

Finalizando este documento, o Quarto Capítulo apresenta a conclusão do trabalho.

2.1 REDES DE COMPUTADORES

A comunicação é um processo dialógico. Em um processo de comunicação, se produz intercâmbio – troca – de informações. Basicamente, uma rede de trabalho é um sistema que permite a comunicação entre pontos distintos, ou seja, um sistema que permite a troca de informações. Os componentes básicos de uma rede de trabalho (ou rede de informações) são um emissor (origem da informação), o meio através do qual a informação trafega (o canal), um receptor (o destino da informação) e finalmente a mensagem, que nada mais é do que a informação em si. Um exemplo comum seria uma pessoa falando no telefone com outra pessoa. O emissor seria quem está falando, o canal seria a linha telefônica, o receptor a pessoa que está ouvindo e a mensagem seria a própria mensagem que está sendo comunicada. Ao longo dos anos as ferramentas para a comunicação de dados foram evoluindo gradativamente, de modo a tornar a troca de informações rápida, fácil e mais eficiente.

A RFC 2828 (*Request for Comments nº 2828 - Internet Security Glossary*) define rede de computadores como uma coleção de hosts interligados para troca de dados. *Host* é definido

2 – REFERENCIAL TEÓRICO

Nesse capítulo, procurou-se descrever os vários aspectos do tema Segurança de Redes de Computadores. Constantemente serão citadas definições retiradas da RFC 2828 (Request for Comments nº 2828 - Internet Security Glossary). As RFCs são documentos produzidos por professores, doutores e pesquisadores nas diversas áreas de tecnologia da informação, que descrevem todos os detalhes das implementações dessas tecnologias, tanto de redes quanto de linguagens, protocolos de comunicações, padrões de funcionamento de hardware, etc. Podem ser consideradas as definições oficiais das tecnologias existentes. Estão disponíveis para consulta pública pela Internet no site www.rfc.net. Especificamente, a RFC 2828 é um Glossário de Segurança na Internet. Nesse tópico procurou-se mostrar as definições dos temas que serão abordados nos tópicos subsequentes: O QUE SÃO REDES DE COMPUTADORES, CLIENTE / SERVIDOR, TCP/IP, INTERNET, SISTEMAS DISTRIBUÍDOS.

2.1 REDES DE COMPUTADORES

A comunicação é um processo dialogal. Em um processo de comunicação, se produz intercâmbio – troca – de informações. Basicamente, uma rede de trabalho é um sistema que permite a comunicação entre pontos distintos, ou seja, um sistema que permite a troca de informações. Os componentes básicos de uma rede de trabalho (ou rede de informações) são um emissor (origem da informação), o meio através da qual a informação trafega (o canal), um receptor (o destino da informação) e finalmente a mensagem, que nada mais é do que a informação em si. Um exemplo comum seria uma pessoa falando no telefone com outra pessoa: O emissor seria quem está falando, o canal seria a linha telefônica, o receptor a pessoa que está ouvindo e a mensagem seria a própria mensagem que está sendo comunicada. Ao longo dos anos as ferramentas para a comunicação de dados foram evoluindo gradativamente, de modo a tornar a troca de informações rápida, fácil e mais eficiente.

A RFC 2828 (*Request for Comments nº 2828 - Internet Security Glossary*) define rede de computadores como uma coleção de hosts interligados para troca de dados. *Host* é definido

pela mesma RFC 2828 como sendo um computador ligado a uma rede de comunicação que possa usar os serviços providos pela rede para trocar dados com outros sistemas interligados. A definição de rede de computadores é utilizada para sistemas de todos os tamanhos e tipos, indo desde a complexa Internet até a um simples computador pessoal interligado remotamente como um terminal de outro computador.

Segundo Tanenbaum (1994), o termo "rede de computadores" pode ser especificado como um conjunto de computadores autônomos, interconectados, sendo capazes de trocar informações. Essa interconexão pode ser feita através de fios de cobre, lasers, microondas, satélites de comunicação e também por fibras ópticas.

Uma rede de computadores baseia-se nos princípios de uma rede de informações, implementando técnicas de *hardware* e *software* de modo a torná-la efetivamente mais dinâmica, para atender às necessidades que o mundo moderno impõe. Redes de computadores incluem todos os equipamentos eletrônicos necessários à interconexão de dispositivos, tais como microcomputadores e impressoras. Esses dispositivos que se comunicam entre si são chamados de nós, estações de trabalho, pontos ou simplesmente dispositivos de rede. Dois computadores, ou nós seriam o número mínimo de dispositivos necessários para formarmos uma rede. O número máximo não é predeterminado, teoricamente todos os computadores do mundo poderiam estar interligados. Entretanto ao conectarmos uma rede em outra (como no caso da Internet) temos que estar certos que somente as informações "públicas" estarão disponíveis. Sofisticados dispositivos devem garantir o sigilo das operações. E mesmo em uma rede privada, fisicamente localizada em um prédio, não podemos permitir que usuários não autorizados acessem dados confidenciais.

Inicialmente as redes foram projetadas com finalidade de pesquisa e o objetivo principal era permitir diversas possibilidades de conectividade entre as partes que estivessem interagindo. Portanto, a interoperabilidade e não a segurança foi enfatizada. Agora, com o crescimento da demanda comercial cada vez mais acentuado, a segurança passou a ser uma necessidade fundamental consistindo foco de discussão das pessoas envolvidas com a tecnologia de redes.

2.1.1 Objetivos das redes de computadores

Tanenbaum (1994) também define os objetivos da interconexão 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-se citar o compartilhamento de uma impressora por vários usuários;

Economia: a substituição gradativa dos antigos mainframes para as redes de computadores de pequeno porte significou uma redução muito grande nos custos de manutenção dos sistemas de informação, possibilitando uma verdadeira revolução nos Cpd's. Esse fenômeno ficou conhecido mundialmente como *Downsizing*. Essas redes de computadores de pequeno porte possibilitam um aumento da capacidade de processamento à 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.

2.1.2 Conjunto de protocolos TCP/IP

O conjunto de protocolos TCP/IP surgiu com a criação de uma rede patrocinada pelo Departamento de Defesa do governo dos Estados Unidos da América (DoD - *Department of Defense*). Uma das tarefas essenciais dessa rede seria manter comunicados, mesmo que apenas uma parte, órgãos do governo e universidades, numa ocorrência de guerras ou catástrofes que afetassem os meios de comunicação daquele país. Dessa necessidade, surgiu a ARPANET, uma rede que permaneceria intacta caso um dos servidores perdesse a conexão.

A ARPANET necessitava então de um modelo de protocolos que assegurasse tal funcionalidade esperada, mostrando-se confiável, flexível e de fácil implementação. É então desenvolvida a arquitetura TCP/IP, que se torna um padrão de fato.

A ARPANET cresceu e tornou-se a rede mundial de computadores - Internet. A utilização (e facilidades) do padrão TCP/IP utilizado pelos fabricantes de outras redes, com a finalidade da conectividade com a Internet.

A normalização do TCP/IP chegou após a sua utilização em massa.

Hoje, quando se menciona TCP/IP, vem imediata a associação com a Internet, ocorrendo de modo idêntico o inverso: a Internet está diretamente relacionada à arquitetura TCP/IP.

O conjunto de protocolos TCP/IP é, na verdade, um grupo de protocolos que trabalham conjuntamente, com o objetivo de estabelecer a comunicação e a transferência de dados entre dois ou mais computadores ligados em rede.

O TCP (*Transmission Control Protocol*), como o próprio nome diz, controla a transmissão dos dados, cuidando para que os dados enviados por um computador cheguem integralmente ao destino correto.

O TCP nada mais é que uma biblioteca de rotinas instaladas nos computadores origem e destino (ou seja, todos os computadores que utilizem o protocolo TCP/IP para se comunicar) que as aplicações como HTTP, *mail*, *Telnet*, e outras, utilizam quando precisam executar o transporte de dados entre hosts.

Para melhor gerenciar a transmissão, o TCP quebra os dados a serem transmitidos em blocos menores, que chamamos de pacotes ou datagramas. Utilizando esta estrutura o TCP é capaz de verificar, se os datagramas chegam ao destino correto ou se não houve perda de dados durante a transmissão, retransmitindo o datagrama se necessário. Fará também o processo inverso, juntando os datagramas no *host* destino para a reconstituição dos dados originais.

Enquanto o TCP cuida da segurança do envio e recebimento dos datagramas, o IP é responsável pela transmissão em si, fazendo o serviço de roteamento, ou seja, conduzindo os dados para os endereços corretos. Na verdade, os dois protocolos se completam: enquanto o IP identifica os endereços e cuida para que os dados sejam enviados pelo meio físicos, o TCP verifica se estes dados enviados foram transmitidos corretamente.

2.1.3 Internet

A Internet originou-se da *Arpanet*, a primeira rede nacional de computadores criada em 1969 pelo Departamento de Defesa do EUA para garantir a segurança em caso de acidente nas comunicações. Esta rede privada era destinada a interligar os computadores dos centros de pesquisa, universidades e instituições militares americanas, permitindo o compartilhamento de recursos entre os pesquisadores que trabalhavam com projetos estratégico-militares.

Em 1972 o governo americano decidiu mostrar o projeto pioneiro à sociedade, e a idéia expandiu-se entre as universidades americanas, interessadas em desenvolver trabalhos cooperativos. Para interligar os diferentes computadores dos centros de pesquisa, em 1980 a Internet adotou o protocolo aberto *TCP/IP* para conectar sistemas heterogêneos, ampliando a dimensão da rede, que passou a falar com equipamentos de diferentes portes, como micros, *workstations*, *mainframes* e supercomputadores.

Somente em 1983, com a separação entre as aplicações para as áreas civil e militar, surgiu definitivamente o nome *Internet*. Três anos depois, a *National Science Foundation* criou uma ligação de alta velocidade com seu centro de supercomputadores e passou a promover a disseminação das informações científicas. Naquela época, o governo americano decidiu financiar a formação de redes regionais em todo o país - uma infra-estrutura com circuitos dedicados e multiplexadores do tipo T1, a 2 Mbps -, o que acabou constituindo a *NSFnet* como uma via expressa para mandar mensagens e arquivos por todo o país. Essa rede, por sua vez, é conectada a outras redes comerciais e públicas que configuram a rede Internet, hoje o principal alicerce das comunicações entre os computadores mundiais.

Com o crescimento da Internet e sua expansão devido à utilização do *TCP/IP*, outras redes perdem sua força. É o caso da *Bitnet*, voltada para a comunicação entre sistemas de grande porte, da *CSnet*, usada pelo pessoal da computação científica e da *UUCP*, que trabalha em ambiente Unix com linhas dedicadas.

O Brasil tem 50.000 pioneiros plugados à Internet. O interesse pela Internet no país ultrapassou os limites acadêmicos e chegou a todos usuários de micros. A demanda é tanta que a Embratel decidiu oferecer, a partir de dezembro de 94, acesso comercial à maior rede de informações do mundo.

A empresa criou um serviço que dará a seus clientes acesso on-line as bases de dados de todo o mundo, com informações de interesse geral como esportes, eventos, espetáculos, previsão meteorológica e sinopses de periódicos. O serviço permitirá também a realização de conferências eletrônicas.

O serviço vai trafegar inicialmente pela *Renpac* e pelo *STM-400* e poderá ser acessado também por grandes corporações quanto pelo usuário de apenas um micro pessoal. O acesso será transparente para usuários do *STM-400*, explica o coordenador do projeto, Hélio Dalgegan, assessor da presidência da Embratel. A empresa vai adotar o correio eletrônico da Internet e já está convertendo o protocolo *SMTP*, que permitirá acesso direto à rede mundial. "O processo comercial muitas vezes envolve valores e dados comerciais que são confidenciais e, por ser muito aberta, a rede não oferece nenhuma garantia de confiabilidade e codificação de dados".

2.2 OS SISTEMAS DISTRIBUÍDOS

Os Sistemas Distribuídos têm, por seu maior objetivo, melhorar a comunicação entre os computadores, ou melhor, propiciar a integração destes num sentido amplo que pode envolver facilidade de mudanças futuras, rapidez nas trocas de informações, confiabilidade na execução dos processos.

Porém, no desenvolvimento de um sistema distribuído encontramos um pequeno problema: *software*. Devido ao elevado tamanho e complexidade de sistemas distribuídos, o seu desenvolvimento exige um conhecimento bastante profundo dessa área e a utilização de técnicas adequadas de concepção e projeto de sistemas.

2.2.1 Aspectos de tolerância a falhas

Pelo fato de sistemas distribuídos possuírem múltiplas partes de *hardware* e de *software* funcionando conjuntamente, as chances de algumas dessas partes falhar é bem maior do que ocorreria num sistema simples.

Um sistema distribuído pode apresentar falhas de vários tipos, dentre as quais aquelas provenientes de defeitos nas linhas de comunicação que interligam os processadores e aquelas referentes a colapsos nos processadores.

Em sistemas tolerantes a falhas, as consequências de defeitos e interferências indevidas pode ser superado através de redundância temporal e/ou redundância física. A redundância temporal corresponde à determinação de um resultado através de execuções repetidas da mesma operação pelo mesmo elemento, usando eventualmente métodos diferentes. A redundância física consiste em ter-se elementos repetidos capazes de executar a mesma operação. Esses elementos referem-se tanto ao *hardware* quanto ao *software* do sistema.

Um sistema, quando não funciona bem, apresenta como consequência resultados incorretos conhecidos por erros. A causa dos erros é a presença de defeitos ou interferências indevidas, conhecidos por falhas, que aparecem tanto a nível de *hardware* quanto de *software*. Ao evento que corresponde ao desvio de comportamento esperado do sistema denominamos falha.

Obviamente, os sistemas tolerantes a falhas vão precisar de considerável redundância do *hardware* e da infra-estrutura de comunicação. Também será necessário a redundância do *software* e mais especificamente dos dados. A replicação de arquivos será uma questão essencial para os futuros sistemas. Os sistemas terão também de ser projetados de maneira a funcionar quando somente parte dos dados estiverem disponíveis, uma vez que a insistência em se ter todos os dados disponíveis todo o tempo não leva a sistemas tolerantes à falhas. Vale observar que o fato de se Ter o sistema indisponível por alguns instantes, hoje considerado aceitável, torna-se cada vez menos razoável, à medida que o computador vai sendo difundido e usado por não-especialistas.

2.2.2 Vantagens e desvantagens

2.2.2.1 Vantagens do sistema distribuído sobre os centralizados

Os sistemas distribuídos oferecem uma economia muito grande, pois os microprocessadores têm uma melhor relação preço/performance do que a oferecida pelos mainframes, por isso a descentralização está caindo continuamente.

Outra razão para se construir sistemas distribuídos é o fato de muitas aplicações serem eminentemente distribuídas. Em um sistema de automação industrial que controla robôs e máquinas ao longo de uma linha de montagem, é interessante que cada robô e cada máquina tenham seu próprio processador. Se todos estes processadores estiverem conectados, teremos um sistema distribuído de automação industrial. No caso de aplicações críticas, como controle de instalações nucleares, ou o controle do tráfego aéreo, o uso de sistemas distribuídos é de fundamental importância.

2.2.2.2 Vantagens do sistema distribuído sobre PCs independentes:

O compartilhamento é a maior vantagem que os sistemas distribuídos tem sobre os PCs independentes, pois o compartilhamento de dispositivos permite que vários usuários tenham acesso a periféricos muito caros, tais como as impressoras laser a cores, as máquinas de fotocomposição, e os dispositivos de armazenamento de alta capacidade, especialmente os óticos, são também candidatos.

Outra razão para se fazer à conexão de um grupo de máquinas isoladas, transformando-as em um sistema distribuído é conseguir melhorar a comunicação entre as pessoas. Como exemplo temos o correio eletrônico, que possui muitos atrativos em relação aos meios de comunicação tradicionais.

2.2.2.3 Desvantagens dos sistemas distribuídos

Apesar das vantagens em relação aos sistemas distribuídos centralizados, existem algumas desvantagens que serão relacionadas neste item.

O primeiro problema está relacionado com a falta de *software* no mercado.

O segundo problema potencial é o das redes de comunicação. Aqui, o ponto principal é a possibilidade de que sejam perdidas mensagens na rede, o que nos obriga a utilizar um *software* especial para fazer a manipulação das mensagens. Outro aspecto relativo às redes é a possibilidade de elas ficarem sobrecarregadas com o tráfego gerado pelo intercâmbio de mensagens.

O terceiro problema está relacionado com a segurança dos dados, pois os dados secretos podem ser acessíveis com grande facilidade.

2.3 SEGURANÇA EM REDES DE COMPUTADORES

O cenário mundial vem passando por grandes transformações nos últimos anos, em diversos aspectos, mais especificamente no que se refere aos aspectos de mercados globais, surgimento de novos mercados e disseminação de informações.

O fator tecnologia tem estado presente a todo o momento, como um dos elementos que possibilita e favorece esse processo, atuando como elemento de difusão, disseminação e compartilhamento de informações, de maneira e velocidade não possíveis até então, atingindo as mais diversas partes do planeta.

Hoje, o mercado global é caracterizado por agilidade e transformação. Essa é uma era, em que a informação é comunicada e o trabalho é conduzido sobre fronteiras, culturas, companhias, indústrias, lugares e funções com novas demandas emergentes em relação a trabalhadores e corporações em todo o mundo.

Hoje muitas transações comerciais podem ser feitas através das redes de computadores. Porém, esta comodidade trouxe a preocupação de que informações confidenciais podem estar expostas a intrusos e atacantes de redes que utilizam meios cada vez mais sofisticados para violar a privacidade e integridade dos dados.

A segurança dos dados é uma questão importante. As falhas de segurança dos ambientes de informática decorrem, normalmente, da falta de compreensão dos aspectos que envolvem a questão. A vulnerabilidade dos sistemas está diretamente ligada à sua própria evolução. O modelo antes usado nos departamentos de informática era baseado num único computador e em alguns terminais fisicamente conectados. A segurança convergia para a proteção e o controle do acesso físico ao computador central e aos terminais. Com a passagem para o modelo descentralizado, começaram a surgir às redes. Os problemas com segurança,

então, aumentaram em função da criação de mais pontos de vulnerabilidade. As características da nova tecnologia contribuíram para isso ao possibilitar a captura de informações que trafegam por linha telefônicas, sua análise, alteração e, até mesmo, a simulação de falsas conexões.

Com a formação de conglomerados empresariais de âmbito mundial, vislumbrou-se a possibilidade de utilizar uma rede de alcance mais amplo, a Internet. Esta serviria não só de meio para a empresa se conectar e trocar informações como também de mecanismo de divulgação e venda de serviços e produtos. A Internet trabalha enviando informações de computador para computador até que as informações cheguem ao seu destino. Quando os dados são enviados de um ponto para outro, todo computador entre eles tem oportunidade de observar o que está sendo enviado. Isso acontece por que o protocolo de comunicação TCP/IP no final da década de 60, tinha como objetivo facilitar o compartilhamento de informações e não previa uma função comercial. Em virtude destas características, apresenta falhas clássicas de segurança.

Os problemas com segurança, então, aumentaram ainda mais, pois os pontos de vulnerabilidade passaram a serem todos os milhões de computadores conectados mundo afora.

Um sistema distribuído pode ser caracterizado como sendo um conjunto de computadores independentes, interligados por uma rede de comunicação, que permite o compartilhamento os diversos recursos do sistema, como *hardware*, *software* e dados. Além disso, o acesso aos recursos deve ser transparente ao usuário, ou seja, independente de sua localização, o usuário deve acessar os serviços da mesma forma, tendo a impressão de que todos os serviços estão em seu computador.

Atualmente, o modelo arquitetural dos sistemas distribuídos mais difundidos é o cliente/servidor, pois ele apresenta uma arquitetura simplificada e flexível, que se adapta às necessidades da maioria dos usuários.

O modelo cliente/servidor é caracterizado pela presença de um ou mais servidores e várias estações de trabalho (clientes). O servidor é responsável pelo gerenciamento e disponibilização dos recursos da rede aos clientes que, por sua vez, realizam pedidos de serviço. É criada uma conexão com o servidor sempre que um cliente solicita um serviço. Além disso, o servidor é capaz de manter várias conexões com vários clientes, simultaneamente.

Cada conexão é feita especificando-se um endereço lógico denominado porta, que identifica o tipo de serviço a ser realizado. Após o recebimento do pedido, o servidor executa o serviço e envia o resultado de volta ao cliente.

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados. A necessidade de proteção deve ser definida em termos das possíveis ameaças e métodos de ataque, e formalizados nos termos de uma política de segurança.

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 segurança perfeita é algo inatingível, segundo a universidade. Portanto, deve-se prevenir ou reduzir a probabilidade de dano ao *hardware*, *software* e aos dados. Esses danos podem ser provenientes de:

- mau uso (acidental ou proposital);
- dano por vandalismo;
- Invasão intencional;
- fraude;
- Sabotagem;
- desastres por fogo, água, terremotos, furacões, etc.

2.3.1 Política de segurança

É definida pela RFC 2828 (Request for Comments nº 2828 - Internet Security Glossary) como sendo o conjunto de regras e práticas que especificam ou regulam como um sistema ou organização provê serviços seguros protegendo os recursos críticos do sistema.



Figura 3— Gráfico de empresas Brasileiras que possui política de segurança – Fonte: Módulo Security

Pode-se comparar a Política de Segurança a Constituição de um país. É ela que deverá coordenar o uso de todos os equipamentos e medidas de segurança da empresa, definindo regras e responsabilidades da segurança da informação.

Uma política de segurança é um instrumento importante para proteger a sua organização contra ameaças a segurança da informação que a ela pertence ou que está a sob sua responsabilidade. Uma ameaça à segurança é comprometida e compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade).

A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação. Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham.



Figura 4 – Gráfico dos tópicos abordados na política de segurança – Fonte: Módulo Security

Além disso a política de segurança estipula penalidades aqueles as quais estão sujeitos aqueles que a descumprem. Antes que a política de segurança seja escrita, é necessário definir a informação a ser protegida.

2.3.2 Tipos de segurança de dados

I - Prevenção: evitar antes que aconteça. Divide-se em:

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

Proteção de arquivos e dados: providenciado 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 do tipo *firewall* cuidam desse aspecto, mantendo a rede protegida contra invasões de usuários não autorizados.

DETECÇÃO: detectar o problema o mais cedo possível. Divide-se em:

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, etc.

Auditoria: periodicamente deve-se analisar os componentes críticos do sistema a 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.

RECUPERAÇÃO: como voltar ao funcionamento normal após um incidente.

Divide-se em:

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.

2.3.3 Propriedades de segurança

As propriedades de segurança de um sistema estão relacionadas à capacidade das entidades acessarem suas informações e recursos (bancos de dados, processadores, impressoras. Etc.) de forma segura. Deve-se entender por entidades o conjunto de pessoas, chaves, processos ou máquinas.

De acordo com Chin (1999), as propriedades que devem ser consideradas no desenvolvimento de um sistema seguro são:

Confidencialidade: apenas as entidades envolvidas podem ter acesso ao conteúdo dos dados que estão trafegando na rede. Qualquer ação de monitoramento da rede não deve ser capaz de ter acesso dos dados.

Integridade: deve-se garantir que a informação transmitida em um ponto é a mesma recebida em outro e que não houve nenhuma adulteração dos dados por parte de terceiros ou de falhas.

Autenticação: as entidades envolvidas em uma comunicação devem ter meios de confirmarem mutuamente suas identidades, certificando-se de com quem estão se comunicando.

controle de acesso: serve para restringir o acesso aos recursos. Assim, apenas entidades autorizadas poderão acessá-los.

2.3.4 Vulnerabilidades de segurança de sistemas baseados em redes

A seguir, apresentamos uma lista das principais vulnerabilidades mais comuns de segurança de sistemas baseados em redes:

1. Controle de acesso a roteador inadequado: ACLs de roteador mal configuradas podem permitir vazamentos de informações através de ICMP, IP, NetBios e levar acesso não-autorizado a serviços dos servidores;

2. Pontos de acesso remoto e não monitorados fornecem um dos meios mais fáceis de acessar uma rede corporativa;
13. Recursos de registro, monitoramento e detecção inadequados em nível de rede e host;
3. Vazamentos de informação podem fornecer a um ataque versões de sistema operacional e aplicativos, usuários, grupos, compartilhamentos, informações de DNS via transferências de zona e serviços em execução através de serviços como SNMP, *finger*, SMTP, *telnet*, *rusers*, *sunrpc* e *NetBios*;
4. *Hosts* rodando serviços desnecessários (tais como *sunrpc*, FTP, DNS, SMTP) deixam portas abertas;
5. Senhas fracas, facilmente adivinháveis e ou reusadas em nível de estação de trabalho podem levar a comprometimento dos servidores;
6. Contas de usuários ou de teste com privilégios excessivos;
7. Servidores da internet mal configurados, especialmente scripts CGI em servidores web e FTP anônimo;
8. ACLs de roteador ou firewall mal configurados podem permitir acesso a sistemas internos diretamente ou quando um servidor da DMZ estiver comprometido;
9. Software sem aplicação de correções (patches), desatualizado, vulnerável ou deixado com as configurações padrão;
10. Controles de acesso a diretórios e arquivos excessivos (compartilhamento do NT/95/98, exportações de NFS do UNIX).
11. Relacionamento de confiança excessivo, tais como Domain Trusts (confianças de domínio) do NT e arquivos *rhosts* e *hosts.equiv* do UNIX podem dar a atacantes acesso não autorizado a sistemas sensíveis;

12. Serviços não autenticados com X Windows;

13. Recursos de registro, monitoramento e detecção inadequados em nível de rede e host;

14. Falta de políticas de segurança, procedimentos, diretrizes padrões básicos mínimos estabelecidos e aceitos.

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados. A necessidade de proteção deve ser definida em termos das possíveis ameaças e métodos de ataque, e formalizada nos termos de uma política de segurança.

Neste capítulo são apresentados objetivos da resposta a incidentes de segurança, a metodologia de resposta para incidentes de segurança, os principais métodos de ataques, as propriedades de segurança que devem ser levadas em consideração durante o desenvolvimento de um sistema seguro e os mecanismos de segurança existentes para preservar as propriedades de segurança e assim, evitar os ataques.

3.1.1 Objetivos da resposta a incidentes de segurança

Nesse tópico enfatizamos os pontos que o profissional de segurança deve seguir para poder definir seus mecanismos de resposta a incidentes de segurança. Os pontos são:

- Confirmar ou descartar a ocorrência de um incidente;
- Promover a acumulação de informações precisas;
- Estabelecer controles para a recuperação e o tratamento adequado das provas;
- Proteger o direito à privacidade estabelecido pela lei e pelas políticas das empresas ou instituições;
- Minimizar a interrupção dos serviços e das operações em redes;
- Permitir retaliações legais e civis contra invasores;
- Apresentar relatórios precisos e recomendações úteis.

Segundo essa metodologia procuramos servir a vários tipos de incidente e de objetivos de resposta.

3. PROBLEMAS E SOLUCOES PARA SEGURANÇA DE REDES DE COMPUTADORES

3.1 CONSIDERAÇÕES INICIAIS

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados. A necessidade de proteção deve ser definida em termos das possíveis ameaças e métodos de ataque, e formalizados nos termos de uma política de segurança.

Neste capítulo são apresentados objetivos da resposta a incidentes de segurança, a metodologia de resposta para incidentes de segurança, os principais métodos de ataque, as propriedades de segurança que devem ser levadas em consideração durante o desenvolvimento de um sistema seguro e os mecanismos de segurança existentes para promover as propriedades de segurança e assim, evitar os ataques.

3.1.1 Objetivos da resposta a incidentes de segurança

Nesse tópico enfatizamos os pontos que o profissional de segurança deve seguir para poder definir seus mecanismos de resposta a incidentes de segurança. Os pontos são:

- Confirmar ou descartar a ocorrência de um incidente;
- Promover a acumulação de informações precisas;
- Estabelecer controles para a recuperação e o tratamento adequado das provas;
- Proteger o direito à privacidade estabelecido pela lei e pelas políticas das empresas ou instituições;
- Minimizar a interrupção dos serviços e das operações em redes;
- Permitir retaliações legais e cíveis contra invasores;
- Apresentar relatórios precisos e recomendações úteis;

Seguindo essa metodologia procuramos servir a vários tipos de incidente e de objetivos de resposta.

3.1.2 Metodologia de resposta a incidentes de segurança

Precisamos seguir alguns passos para solucionarmos ou prevenirmos problemas de segurança, propomos seguir as etapas abaixo:

- Preparação pré-acidente: Tomar medidas para preparar-se antes que um acidente ocorra;
- Detecção de incidentes: Saber da suspeita de um incidente de segurança;
- Resposta inicial: Realizar uma investigação inicial. Obter as provas mais voláteis (inclusive o testemunho humano) e confirmar se um incidente ocorreu ou não;
- Estratégia de formulação de resposta: Com base nos resultados de todos os fatos conhecidos, determinar a melhor resposta e obter a aprovação da direção da empresa ou instituição;
- Duplicação (*backup* periciais): Decidir a necessidade de criar imagens periciais físicas para fins de investigação ou realizar uma coleta de provas on line;
- Investigação: Cumprir as demoradas etapas de investigação para determinar o que aconteceu, quem foi o responsável e como evitar que o fato volte a repetir-se;
- Implementação de medidas de segurança: Proteger ativamente os sistemas atacados, aplicando medidas de segurança para isolar e conter o incidente;
- Monitoração da rede: Monitorar as atividades da rede para investigar e garantir a segurança da rede atacada;
- Recuperação: Devolver o sistema atacado a um estado operacional seguro;
- Geração de relatórios: Documentar com precisão todos os detalhes da etapa de investigação e das medidas de segurança a serem tomadas;
- Finalização: Analisar os processos conduzidos, registrar as lições aprendidas e resolver os problemas que possam surgir;

Figura 5 – Diagrama de resposta a incidentes de segurança

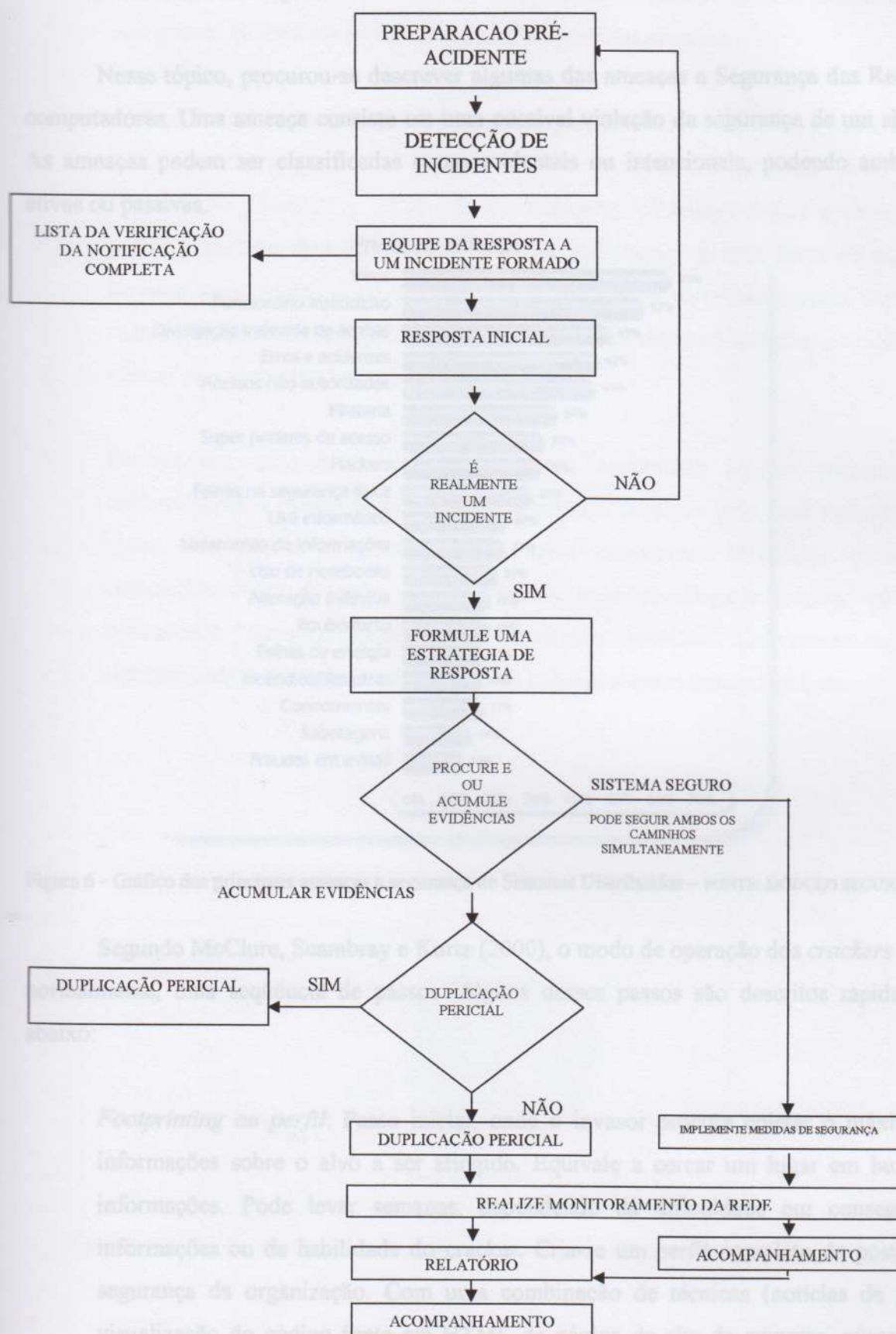


Figura 5 – Diagrama de resposta a incidentes de segurança

3.1.3 Métodos de ataque

Nesse tópico, procurou-se descrever algumas das ameaças a Segurança das Redes de computadores. Uma ameaça consiste em uma possível violação da segurança de um sistema. As ameaças podem ser classificadas como acidentais ou intencionais, podendo ambas ser ativas ou passivas.

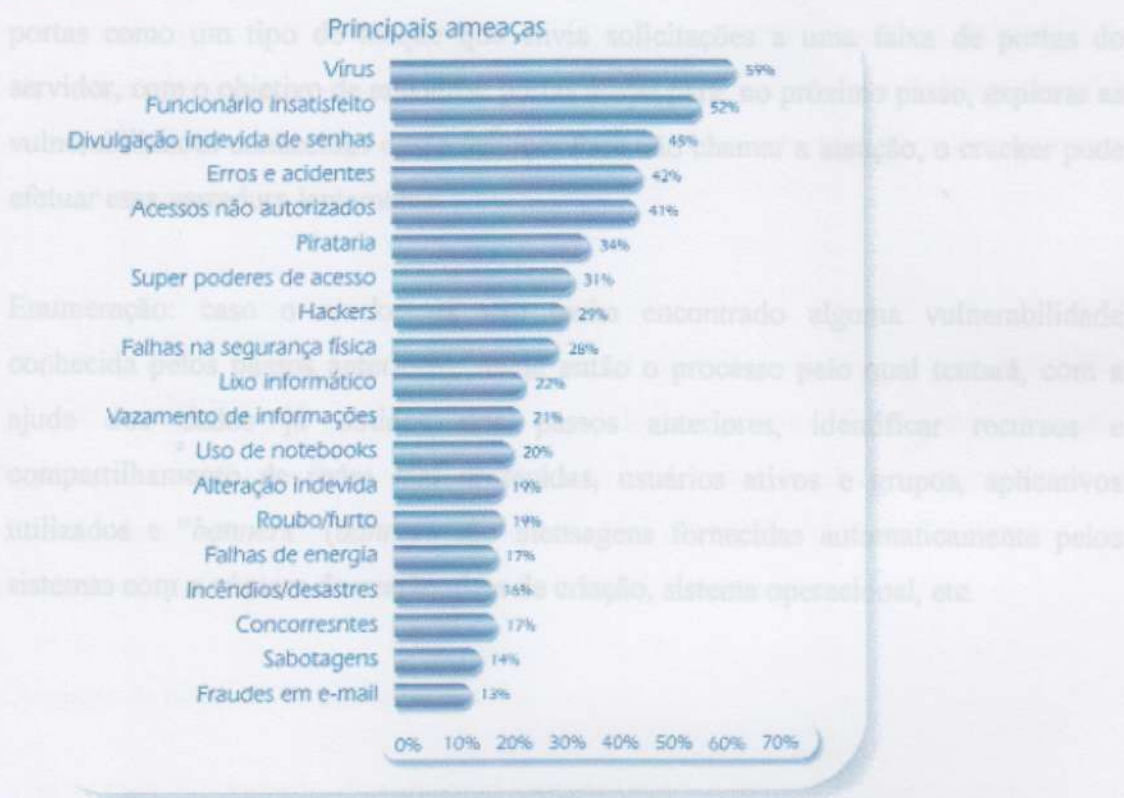


Figura 6 - Gráfico das principais ameaças a segurança de Sistemas Distribuídos – FONTE: MÓDULO SECURITY

Segundo McClure, Scambray e Kurtz (2000), o modo de operação dos *crackers* segue, normalmente, uma seqüência de passos. Alguns desses passos são descritos rapidamente abaixo:

Footprinting ou perfil: Passo inicial, onde o invasor procura coletar o máximo de informações sobre o alvo a ser atingido. Equivale a cercar um lugar em busca de informações. Pode levar semanas, dependendo da dificuldade em conseguir as informações ou da habilidade do cracker. Cria-se um perfil completo da postura de segurança da organização. Com uma combinação de técnicas (notícias de jornal, visualização do código fonte em HTML da página do site da empresa, números de

telefone, etc.) e ferramentas de software, atacantes podem adquirir informações de uma grande quantidade de fontes, traçando o perfil da empresa.

Varredura: processo pelo qual o invasor, depois de escolhido o alvo, passa a verificar todas as portas e “janelas” a procura de sistemas ativos e alcançáveis. A RFC 2828 (*Request for Comments nº 2828 - Internet Security Glossary*) define a varredura de portas como um tipo de ataque que envia solicitações a uma faixa de portas do servidor, com o objetivo de encontrar portas ativas para, no próximo passo, explorar as vulnerabilidades conhecidas desse serviço. Para não chamar a atenção, o cracker pode efetuar essa varredura lentamente.

Enumeração: caso o cracker já não tenha encontrado alguma vulnerabilidade conhecida pelos passos anteriores, inicia então o processo pelo qual tentará, com a ajuda dos dados já obtidos nos passos anteriores, identificar recursos e compartilhamento de redes mal protegidas, usuários ativos e grupos, aplicativos utilizados e “banners” (*banners* são mensagens fornecidas automaticamente pelos sistemas com o número de versão, data de criação, sistema operacional, etc.

3.2.3- Ataques de negação de serviço

Um ataque de negação de serviço é caracterizado por uma tentativa explícita dos atacantes em impedir o acesso a um recurso de rede. A tentativa de um flood (inundação) em uma rede, dificultando o legítimo tráfego, é uma tentativa de negação de serviço. Outro exemplo é a tentativa de um flood (inundação) em uma rede, dificultando o legítimo tráfego, é uma tentativa de negação de serviço. Outro exemplo é a tentativa de um flood (inundação) em uma rede, dificultando o legítimo tráfego, é uma tentativa de negação de serviço.

Nem todo serviço negado, no entanto, resulta de atividades maliciosas. Outros tipos de ataque podem incluir uma tentativa de negação de serviço.

Figura 7- Gráfico dos principais responsáveis por problemas com segurança – Fonte: Módulo Security

Responsáveis pelos problemas com segurança



3.2 MECANISMOS DE ATAQUE:

Neste capítulo são apresentados os principais métodos de ataque:

3.2.1 Sniffing ou “farejar”

Definido pela RFC 2828 (Request for Comments nº 2828 - Internet Security Glossary) como sendo o ato de escutar passivamente os dados de uma rede, a procura de senhas de acesso. O sniffer é um programa ou dispositivo que analisa tráfego de rede. Sniffers são úteis para gerenciamento de redes, mas nas mãos crackers permitem roubar senhas e outras informações sigilosas.

3.2.2 Spoofing ou “fingimento”

Spoofing é o ato de usar uma máquina para personificar outra. Isso é feito forjando o endereço de origem de um ou mais hosts empenhados na autenticação das máquinas individualmente. Se há interfaces de rede entre o atacante e o alvo, o atacante estará desperdiçando tempo (Por exemplo, se os pacotes têm de cruzar um hub inteligente, uma ponte ou um roteador, o spoofing provavelmente falhará).

3.2.3 Ataques de negação de serviço

Um ataque de negação-de-serviço é caracterizado por uma tentativa explícita dos atacantes em impedir que os usuários de um determinado serviço possam usá-lo. A título ilustrativo desse tipo de ataque, pode-se citar: 1) a tentativa de um *flood* (inundação) em uma rede, dificultando o legítimo tráfego da mesma; 2) tentativa de rompimento de conexões entre duas máquinas, dificultando o acesso a um serviço; 3) tentativa de impedimento de acesso a um serviço por parte de um usuário e 4) tentativa de romper serviços a um sistema específico, ou a um usuário.

Nem todo serviço negado, mesmo aqueles que resultam de atividades maliciosas são necessariamente ataques de negação-de-serviço. Outros tipos de ataque podem incluir uma negação-de-serviço como um componente, mas, a negação-de-serviço pode ser parte de um ataque maior. O uso ilegítimo de recursos também pode resultar em negação-de-serviço. Um

usuário intruso pode usar a área de ftp anônimo como um lugar para armazenar cópias ilegais de software comercial, consumindo espaço em disco e gerando tráfego de rede.

3.2.3.1 Falhas de protocolo

Gera uma família de ataques chamados DoS (negação de serviço), os *hosts* atacados ou reinicializa ou tem a sua performance prejudicada.

3.2.3.2 Smurf

O *smurf* é outro tipo de ataque de negação de serviço. O agressor envia uma rápida de solicitações Ping (um teste para verificar se um serviço da Internet esta acessível) para um endereço de broadcast. Usando spoofing, o cracker faz com que o servidor de broadcast encaminhe as respostas não para seu endereço, mas para o da vítima. Assim o computador-alvo é inundado pelo Ping.

3.2.3.3 Interrupção de serviço

Os ataques de interrupção de serviço geralmente desativam um ou mais serviços de rede. Se sofrer este tipo de ataque, você pode ser forçado a reinicializar ou reiniciar vários serviços. E, embora isso não seja um risco importante de segurança, tempo de paralisação (*downtime*) pode ser valioso. É um ataque praticamente sem defesa.

3.2.3.4 Denial of service(dos)

Ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Há muitas variantes como os ataques distribuídos de negação de serviço (DDoS) que paralisam vários sites ao mesmo tempo. Nessa variante, o agressor invade muitos computadores e instala neles um *software zumbi*, como o *Tribal Flood* ou o *Trinoo*. Quando recebem a ordem para iniciar o ataque, os zumbis bombardeiam o servidor alvo, tirando-o do ar.

3.3.3.5 Ping of death (ping da morte), flooding (inundação), smurfing, denial of service (negação de serviço):

A RFC 2828 (*Request for Comments nº 2828 - Internet Security Glossary*) define esses tipos de ataques como sendo a tentativa de causar falha em um sistema de computador conectado a Internet pelo excesso de dados de entrada (mais do que o sistema pode processar), causando a sua parada ou lentidão excessiva. Não possui a finalidade de invadir uma rede ou roubar informações de dentro dela e sim de parar o funcionamento da rede. Cross (2000) descreve esse tipo de ataque como um esmagamento de um computador que provê serviços a Internet. Complementa, definindo-os como muito difíceis de prevenir, pois exploram uma falha na tecnologia básica da comunicação da Internet. Cada uma das variantes explora um tipo de vulnerabilidade específico de cada comando ou do protocolo. Por exemplo, o ataque *Ping of Death* utiliza o comando ping comum em redes (comando que verifica se um host ou computador está “no ar”), modificando o tamanho do pacote enviado, causando inundação de dados no computador destino, tirando-o do ar. Uma variante do *Denial of Service*, são os temidos *DDOS (Distributed Denial of Service)*, onde segundo Fithen (2000), é um tipo de ataque complexo, não possuindo soluções fáceis.

3.2.4 VÍRUS

Os vírus propagam-se de várias maneiras: por disquetes infectados, por downloads feitos na Internet, executando-se arquivos anexos de *e-mail* e, ultimamente, apenas lendo-se um e-mail infectado.

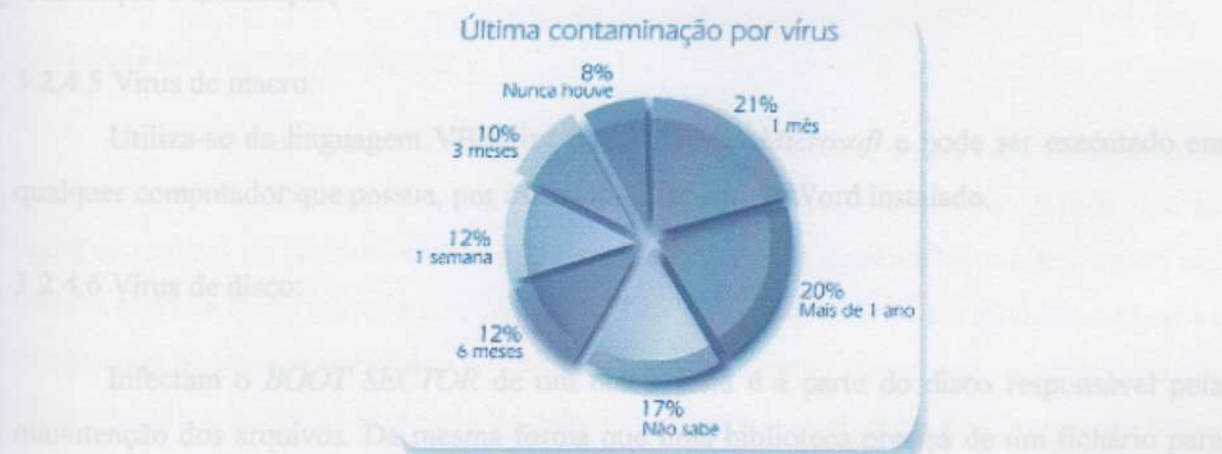


Figura 8 – Gráfico da contaminação por vírus em Empresas Brasileiras - Fonte: Módulo Security

Os principais tipos são:

3.2.4.1 Vírus simples

É 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;

3.2.4.2 Cavalo de tróia ou *trojan*

É um programa que aparenta ter uma função útil, mas possui alguma função maliciosa que burla os mecanismos de segurança. Não possui a capacidade de se auto replicar. Como exemplo pode-se citar um jogo puxado pela Internet, que na verdade, ao ser executado, tira a atenção do usuário enquanto executa algum dano ao computador ou seus dados em segundo plano;

3.2.4.3 *Worm* ou “verme”

É um programa de computador que pode se executar independentemente, propagar-se pelos computadores de uma rede sozinho, podendo consumir os recursos dos computadores destrutivamente;

3.2.4.4 Vírus polimorfo:

Tipo de vírus que modifica a si mesmo à medida que se dissemina, dificultando a sua localização e eliminação;

3.2.4.5 Vírus de macro:

Utiliza-se da linguagem VBScript dos *softwares Microsoft* e pode ser executado em qualquer computador que possua, por exemplo, o aplicativo Word instalado.

3.2.4.6 Vírus de disco:

Infectam o *BOOT SECTOR* de um disco. Esta é a parte do disco responsável pela manutenção dos arquivos. Da mesma forma que uma biblioteca precisa de um fichário para saber onde se encontram os livros, um disco precisa ter uma tabela com o endereço dos dados armazenados. Qualquer operação de entrada e saída (carregamento ou salvamento de um

arquivo, por exemplo), precisaria do uso dessa tabela. Salvar ou carregar um arquivo num disco flexível infectado possibilitaria a ativação do vírus, que poderia infectar outros discos flexíveis e o disco rígido.

3.2.4.7 Vírus companheiros

Criam um arquivo com o mesmo nome de um arquivo.EXE presente no disco, só que com extensão.COM. Quando é digitado um nome de um programa no prompt do DOS sem a extensão, primeira o sistema operacional vai procurar por um programa cuja extensão seja.COM, se não achar, ele tentará achar um com extensão.EXE e, caso não encontre, procurará por um com extensão.BAT. Conclusão, o vírus será executado primeiro e depois de executar alguma tarefa, o vírus chamará o programa original.

Com relação à *forma de atuação*, podemos citar os seguintes vírus:

Residentes e não residentes: Os vírus do tipo residente são aqueles que permanecem na memória após a execução de um programa infectado. Enquanto ele estiver carregado na memória, todos os programas executados durante este período serão infectados. Não residentes atuam apenas quando executados.

Residentes temporariamente: Permanecem na memória principal por um determinado tempo (ou até infectar um ou mais arquivos) e depois retira-se da memória passando a agir como um vírus não residente.

3.2.5 Back door - porta dos fundos

Back door é um mecanismo que provê acesso a um sistema e seus recursos através de um procedimento diferente do usual. *backdoors* são portas abertas por default que às vezes(ou muitas) os administradores de sistema esquecem de desativá-las e assim temos um sistema aberto a quem quiser entrar. A maneira melhor se prevenir é sem dúvida atualizar as versões dos programas instalados no computador. Um detalhe importante: programas Anti-Vírus não são capazes de descobrir Backdoors, somente a atualização dos programas é que podem eliminar em definitivo este problema.

3.2.6 Cracker de senha - *password cracking*

Um *cracker* de senha é qualquer programa que supera a segurança de senha revelando senhas que foram criptografadas. Entretanto isto não significa que cracker de senha possa necessariamente descriptar qualquer coisa.

Atividade de descobrir passwords. O método mais comum é o das tentativas, de nome técnico *Brute-Force Attack*. Passa por arranjar um dicionário de palavras possíveis para passwords com a sua respectiva palavra cifrada e o programa que tenta encontrar cada password desconhecida no dicionário. Estes dicionários e programas costumam já existir em sites especiais para hackers. Dois dos mais conhecidos programas do gênero é o *Crack* e o *CrackJack*.

O processo consiste em deixar o programa a procurar no dicionário cada *password* cifrada, para obter a sua forma original, ou seja, não cifrada.

3.4 MECANISMOS DE DEFESA

Existem para dar segurança a sistemas distribuídos diversos mecanismos de defesa, vamos ver a seguir os mais adotadas:



Figura 9 – Gráfico das principais medidas de segurança adotadas – Fonte: Módulo Security

3.4.1 Criptografia

A RFC 2828 (*Request for Comments nº 2828 - Internet Security Glossary*) define o termo criptografia como a ciência matemática que lida com a transformação de dados para mudar seu significado em algo ininteligível para o inimigo, isto é, esconder o seu conteúdo semântico, prevenindo sua alteração ou seu uso sem autorização.

A Criptografia tem suas origens há muitos anos. Comenta-se que o imperador Romano Júlio César teria sido o primeiro a empregá-la quando enviava cartas criptografadas, pois 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 à 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.

Hoje a Criptografia utiliza técnicas muito mais complexas que as de César Augusto mais a sua idéia ainda é empregada.

A criptografia é um método utilizado para modificar um texto original de uma mensagem a ser transmitida (texto normal), gerando um texto criptografado na origem, através de um processo de codificação definido por um método de criptografia. O texto criptografado é então transmitido e, no destino, o inverso ocorre, isto é, o método de criptografia é aplicado agora para decodificar o texto criptografado transformando-o no texto original.

Existem também a criptografia que utiliza uma chave de codificação. Isto é, para um mesmo texto normal e um mesmo método de criptografia, chaves diferentes podem produzir textos criptografados diferentes.

Criptografia com Chaves Secretas (ou Simétricos)

Este método de criptografia consiste em substituir as letras de uma mensagem pela *n*-ésima letras após a sua posição no alfabeto. Assim o texto criptografado produzido para um

mesmo texto normal pode variar de acordo com o valor de n , que é a chave utilizada nos processos de codificação e decodificação do método.

Data Encryption Standard (DES): é um dos principais métodos de criptografia baseada em chave secreta. Foi desenvolvido pela IBM e adotado pelo governo do EUA como método de criptografia padrão.

O método DES codifica blocos de 64 bits de texto normal gerando 64 bits de texto criptografado. O algoritmo de codificação é parametrizado por uma chave K de 56 bits e possui 19 estágios diferentes.

Criptografia com chave Pública (Assimétricos)

Este método de criptografia baseia-se na utilização de chaves distintas: uma para codificação (E) e outra para a decodificação (D), escolhidas de forma que a derivação de D a partir de E seja em termos práticos, senão impossível, pelo menos difícil de ser realizada.

Uso de criptografia em redes

Podemos então garantir uma comunicação segura na rede através da implantação de criptografia. Podemos, por exemplo, implantar a criptografia na geração dos pacotes, ou seja, apenas as mensagens enviadas de máquina para máquina serão criptografadas. O único problema disso continua sendo a escolha das chaves. Se implementarmos criptografia com chave simples (uma única para criptografar e decriptografar) temos o problema de fazer com que todas as máquinas conheçam esta chave, e mesmo que isso possa parecer fácil em uma rede pequena, redes maiores que não raramente atravessam ruas e avenidas ou mesmo bairros isto pode ser inviável. Além disso, talvez queiramos estabelecer conexões confiáveis com máquinas fora de nossa rede e não será possível estabelecer uma chave neste caso e garantir que somente as máquinas envolvidas na comunicação a conheçam.

Se, contudo, criptografar-mos as mensagens com chave pública e privada, temos o problema de conhecer todas as chaves públicas de todas as máquinas com quem queremos estabelecer comunicação. Isto pode ser difícil de controlar quando são muitas.

3.4.2 Kerberos

Kerberos é um serviço de autenticação distribuída desenvolvido no MIT (*Massachusetts Institute of Technology*) que permite um parceiro provar sua identidade perante um outro parceiro sem enviar dados confidenciais pela rede. Esse processo é realizado como um serviço de autenticação terceiro parceiro confiável utilizando criptografia convencional.

O Kerberos utiliza criptografia para provar a identidade do usuário manipulando dois tipos de chave:

- Chave secreta do usuário - chave conhecida apenas pelo usuário e pelo Kerberos com a finalidade de autenticar o usuário ao Kerberos; deverá existir uma etapa anterior em que serão cadastrados os clientes e suas chaves secretas ficando armazenadas na Base de Dados do Kerberos;

- Chave de sessão - chave gerada pelo Kerberos após ter autenticado o usuário e tem por objetivo autenticar o intercâmbio realizado por um determinado par de usuários que definem uma sessão; a chave é gerada atendendo a uma solicitação feita por um dos usuários, sendo válida por um tempo pré-determinado e conhecida apenas pelos dois parceiros para os quais ela foi originalmente gerada.

3.4.3 Firewall

A RFC 2828 (*Request for Comments nº 2828 - Internet Security Glossary*) define o termo *firewall* como sendo uma ligação entre redes de computadores que restringem o tráfego de comunicação de dados entre a parte da rede que está “dentro” ou “antes” do *firewall*, protegendo-a assim das ameaças da rede de computadores que está “fora” ou depois do *firewall*. Esse mecanismo de proteção geralmente é utilizado para proteger uma rede menor (como os computadores de uma empresa) de uma rede maior (como a Internet).

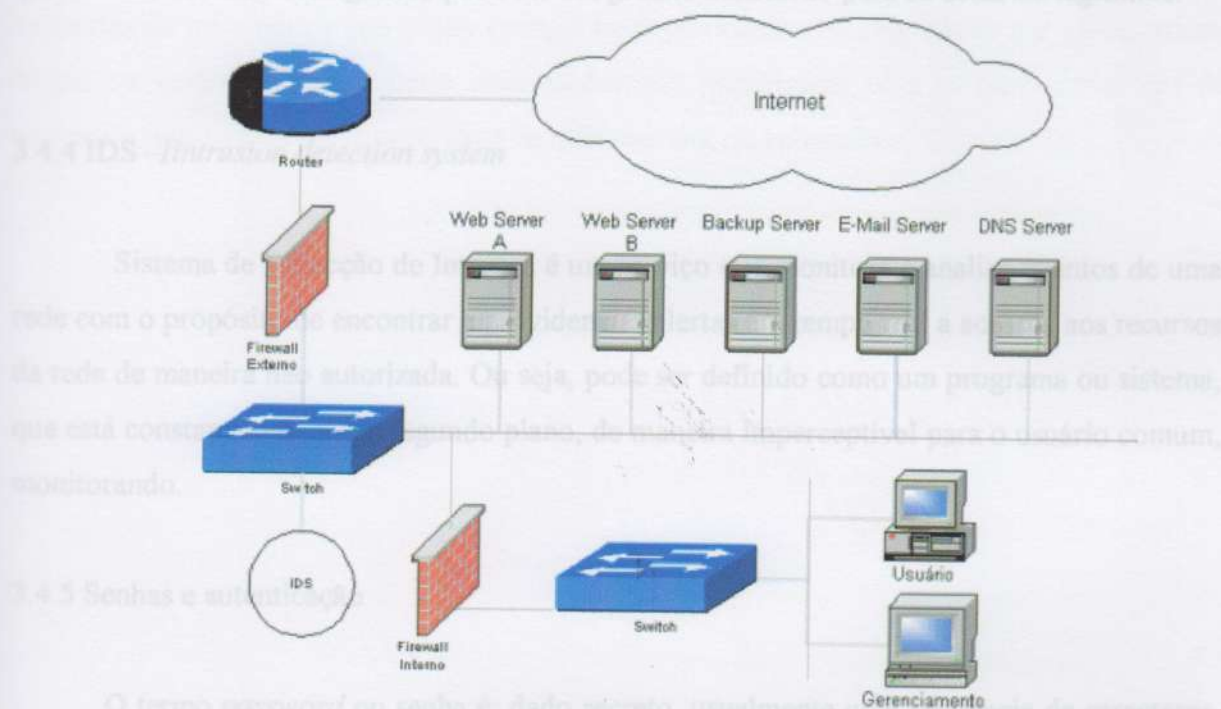


Figura 10 – Modelo de Firewall

Já mencionamos que em redes privadas geralmente são estabelecidos regimes de confiança mútua, ou seja, se quem esta me enviando a mensagem é a máquina "X" então posso aceitá-la, pois eu "confio" na máquina "X" e sei que nenhuma mensagem maliciosa virá dela. Sabemos também que o endereço de uma máquina pode ser facilmente falsificado. Neste caso, fica muito fácil a um intruso enviar mensagens de qualquer lugar dizendo ser a máquina "X". Um *firewall* pode resolver facilmente este problema: ao receber um pacote de fora da minha rede, ele verifica qual o endereço de origem e de destino, não permitindo entrar ou sair pacotes cujos endereços de origem e destino pertençam à mesma rede. Mas ele pode fazer muito mais que isto.

Um *firewall* pode ser configurado mais rigorosamente, dependendo da necessidade da rede. Alguns são capazes até de bisbilhotar o conteúdo dos pacotes, procurando, por exemplo, códigos de vírus, mas essa idéia não é prática, pois teríamos um "gargalo" nele. Pode-se, por exemplo, configurá-lo para não aceitar comunicações somente para determinados serviços (ftp, por exemplo) ou simplesmente não aceitar nenhuma comunicação. Neste caso uma máquina da sub-rede deverá estabelecer esta comunicação e nunca uma de fora. Vemos então que um firewall mal configurado pode ser um grande transtorno para os usuários legítimos.

3.4.4 IDS – *Intrusion detection system*

Sistema de Detecção de Intrusos é um serviço que monitora e analisa eventos de uma rede com o propósito de encontrar e providenciar alertas em tempo real a acessos aos recursos da rede de maneira não autorizada. Ou seja, pode ser definido como um programa ou sistema, que está constantemente, em segundo plano, de maneira imperceptível para o usuário comum, monitorando.

3.4.5 Senhas e autenticação

O termo *password* ou senha é: dado secreto, usualmente uma seqüência de caracteres, que é usado como informação para autenticar um usuário ou pessoa. Esclarece também que, normalmente, é utilizada em conjunto com uma identificação do usuário no processo de autenticação, quando da entrada do usuário na rede ou sistema.

Autenticação é o processo de verificar a identidade declarada por uma entidade do sistema, ou seja, verificar se, quem está tentando utilizar o sistema ou ganhar acesso, é realmente quem declara ser.

3.4.6 Antivírus

Esses *software s* possuem uma base de dados com as assinaturas dos vírus conhecidos. Essas assinaturas são o código dos vírus, que são verificados arquivo por arquivo no processo de procura.

O ponto chave é manter a base de dados atualizada com as assinaturas de todos novos vírus descobertos a cada dia. Deve-se atualizar o *software* antivírus frequentemente, a fim de manter-se protegido.

3.4.7 Alertas

Os Alertas são patches distribuídos ou pelas comunidades de segurança tipo *CERT* ou empresas de informática que visam corrigir bugs produzidos ou explorados por vírus, worm, trojan ou vulnerabilidades. Estas informações são importantes para os administradores de sistema e responsáveis pela segurança de qualquer site ou aplicação.

	Sistemas de detecção de intrusões (IDS - <i>Intrusion Detection System</i>) podem avisar os administradores de sistema via e-mail, via mensagens no terminal do administrador, etc; SOFTWARE: Genius 2.0: www.sinnorx.com/genius BlackIce: www.networkice.com Check Promiscuous Mode: www.info.cert.org
Spoofing ou "fingimento"	Utilizar um Firewall bem configurado; Criptografar todas as informações; A maneira melhor é sem dúvida atualizar as versões dos programas instalados no computador. O Fabricante está sempre pronto a avisar e prover uma nova versão corrigida do programa quando é descoberto um Backdoor. Inclusive os patches de atualização são uma boa prática; Sempre que possível desative a capacidade RIPv1 dos roteadores;

3.4.8 TABELA RESUMO DE ATAQUES E CONTRAMEDIDAS - DEFESA

TIPOLOGIA DE ATAQUE	CONTRAMEDIDAS - DEFESA
Sniffing ou “farejar”	Sistemas de detecção de intrusos (IDS - <i>Intrusion Detection System</i>) 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, etc.; SOFTWARE: Genius 2.0: www.sinnerz.com/genius BlackIce: www.networkice Check Promiscuos Mode: www.info.cert.org
Spoofing ou “fingimento”	Utilizar um Firewall bem configurado; Criptografar todas as informações; A maneira melhor é sem dúvida atualizar as versões dos programas instalados no computador. O Fabricante está sempre pronto a avisar e prover uma nova versão corrigida do programa quando é descoberta um Backdoor. Inclusive os patches de atualização são uma boa prática; Sempre que possível desative a capacidade RIPv1 dos roteadores.

TIPOLOGIA DE ATAQUE	CONTRAMEDIDAS - DEFESA
<i>Smurf</i>	Utilizar um Firewall bem configurado; Criptografar todas as informações;
<i>Denial of service(dos)</i>	Algumas regras podem ser estabelecidas no desenvolvimento de um IDS para que este seja menos vulnerável a tais ataques, são elas: • Verificar todos os checksums; • Examinar corretamente os cabeçalhos; • Verificar existencia de flags, SYN, ACK, RST, etc. • Realizar corretamente a remontagem de pacotes; • IDS deve conhecer a topologia da rede; • IDS deve conhecer os sistemas instalados; • IDS deve conhecer a configuração dos sistemas; • Desabilitar os serviços desnecessários; • Utilizar controle de acesso através de ferramentas como o tcp_wrappers, instalar e configurar um firewall entre sua rede local e redes externas (geralmente entre sua rede local e a Internet); • É também importante analisar constantemente os logs e a integridade de arquivos importantes do sistema.

TIPOLOGIA DE ATAQUE	CONTRAMEDIDAS - DEFESA
VÍRUS	Um bom anti-vírus, atualizado periodicamente, e muito bom senso ainda são as melhores maneiras de se proteger. Os mesmos autores classificam a política de segurança para os vírus em três aspectos: • Prevenção: tenta evitar a contaminação de qualquer arquivo da organização; • Detecção: tenta detectar, o mais rápido possível, a contaminação de algum arquivo; • Remoção: tenta remover o vírus do sistema infectado, que pode ser feito através de deleção do arquivo, eliminação do vírus ou reinstalação do Sistema SOFTWARES Norton – Antivírus ; VirusScam

TIPOLOGIA DE ATAQUE	CONTRAMEDIDAS - DEFESA
Back door - porta dos fundos	Criptografar todas as informações; A maneira melhor é sem dúvida atualizar as versões dos programas instalados no computador. O Fabricante está sempre pronto a avisar e prover uma nova versão corrigida do programa quando é descoberta um Backdoor. Inclusive os patches de atualização são uma boa prática. Um detalhe importante: programas Anti-Vírus não são capazes de descobrir Backdoors, somente a atualização dos programas é que podem eliminar em definitivo este problema. Programas de Firewall pessoal, no entanto, podem ser úteis para amenizar (mas não eliminar) este tipo de problema. SOFTWARES: SEM-NOSadmin 5.0: www.bindview.com; Hidden Object Locator: www.netwarefiles.com Kane Security Analiyst: www.intrusion.com

CONCLUSÃO

TIPOLOGIA DE ATAQUE	CONTRAMEDIDAS - DEFESA
Cavalo de tróia ou trojan	sofrem uma evolução contínua. Na área de segurança Criptografar todas as informações; Utilizar um Firewall bem configurado; Existem no entanto medidas preventivas que minimizam os problemas trazidos com os e-mails: 1. Desligue a opção de "autoexecução" dos programas anexados ao e-mail; 2. Desligue a opção de "auto-abertura" dos arquivos anexados aos e-mails; 3. Desligue as opções de execução de programas Java e do JavaScript. Todos estes itens evitam a propagação automática dos Vírus e Cavalos de Tróia.
SITES DE SEGURANÇA	
http://www.cert.org/advisories/; http://www.cert.org/current/current_activity.html; http://online.securityfocus.com/; http://www.incidents.org/. http://www.microsoft.com/technet/security http://www.zdnet.com http://www.modulosecurity.com.br	

CONCLUSÃO

Todas as coisas de uma forma geral sofrem uma evolução contínua. Na área da tecnologia a visão desta evolução é mais fácil de ser notada. As técnicas em segurança evoluem e os ataques também, mas a atenção dada à questão da segurança dos sistemas ainda não é a necessária, as pessoas realmente só se preocupam em assegurar suas informações quando seus sistemas já foram de alguma forma invadidos.

É preciso também levar em consideração que apenas hardware e software disponíveis no mercado atualmente não são suficientes para assegurar os dados de uma rede que se conecte a Internet. Os profissionais envolvidos com a questão de segurança devem traçar um projeto para implantação de um sistema de segurança completo.

Este sistema de segurança deve contar com uma Política de Segurança adequada às necessidades da rede, para que trabalhe em conjunto com o *software* escolhido, desta forma envolvendo todas as pessoas - principalmente os usuários - que trabalhem com esta rede para que adotem os procedimentos de Segurança determinado por esta Política, fazendo assim valer a aquisição de um *software* especial para assegurar suas informações. Nenhum método, porém, é completamente seguro e a prova de violações. Mesmo os algoritmos mais complexos de criptografia, que levariam séculos para serem quebrados por força bruta no melhor computador existente, estão sensíveis a falhas, seja na troca das chaves ou na arquitetura do próprio algoritmo. O fenômeno da expansão dos serviços de redes como a Internet e a *World Wide Web* obrigam que a segurança e a encriptação se tornem cada vez mais importantes. Haverá um aumento das transações computadorizadas e do comércio eletrônico. O dinheiro eletrônico necessitará de encriptação para proteger o anonimato e a privacidade dos usuários.

O fundamental é que não devemos nos preocupar em apenas construir sistemas de informação maiores, mais rápidos e melhores. Devemos, sim é enfrentar o desafio de implantarmos políticas de segurança que nos ajudem a construir sistemas mais eficazes e seguros.

GLOSSÁRIO

A

ActiveX *para Cliente Servidor (Client/Server)*

Componentes utilizados para permitir a conexão via objetos ativos, com aplicações do lado servidor.

Agent

Um programa de computador ou processo que opera sobre uma aplicação cliente ou servidor e realiza uma função específica, como uma troca de informações.

Algoritmo Assimétrico (*Asymmetric Algorithm*)

É um algoritmo de criptografia que usa duas chaves: uma chave pública e uma chave privada, onde a chave pública pode ser distribuída abertamente enquanto a chave privada é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave. Também conhecido como algoritmo de chave pública..

Algoritmo Simétrico (*Symmetric Algorithm*)

Algoritmo de criptografia que usa somente uma chave, tanto para criptografar como para descriptografar. Esta chave deve ser mantida secreta para garantir a confidencialidade da mensagem. Também conhecido como algoritmo de chave secreta.

ANSI (American National Standards Institute)

- 1 - Uma organização afiliada à ISO e que é a principal organização norte-americana envolvida na definição de padrões (normas técnicas) básicos como o ASCII.
- 2 - Conjunto de normas para a transferência de caracteres de controle. Utilizado para tratamento de atributos, cores, endereçamento do cursor, etc, em terminais ou emuladores de terminais.

ARPANET

Advanced Research Projects Agency Network. Rede de longa distância criada em 1969 pela Advanced Research Projects Agency (ARPA, atualmente Defense Advanced Projects Research Agency, ou DARPA) em consórcio com as principais universidades e centros de pesquisa dos EUA, com o objetivo específico de investigar a utilidade da comunicação de

dados em alta velocidade para fins militares. É conhecida como a rede-mãe da Internet de hoje e foi colocada fora de operação em 1990, posto que estruturas alternativas de redes já cumpriam seu papel nos EUA.

Ato de verificar a identidade de um usuário, de dispositivo, ou de outra entidade em um sistema computacionalizado, frequentemente como um pré-requisito e permitir o acesso aos recursos em um sistema.

Arquitetura Cliente Servidor (Client/Server)

Authentication Token (Dispositivo de Autenticação)

É toda arquitetura de rede onde estações (microcomputadores) executam aplicações clientes que se utilizam de programas servidores para transferência de dados do próprio servidor ou comunicação com outras estações e suas aplicações clientes.

Ataque

ASCII (American Standard Code for Information Interchange)

Autorização

Código numérico usado para representar caracteres em arquivos texto em computadores e dispositivos de armazenamento eletrônico de dados.

Ato de tentar entrar ou danificar um sistema, desviando-se dos seus controles de segurança.

Um ataque pode buscar a obtenção de informações privilegiadas, a sua alteração ou a sua indisponibilização. O sucesso de um ataque depende da vulnerabilidade do sistema (vítima), da atividade e da eficácia de contramedidas existentes.

Ataque

Ataque que aproveita transações, procedimentos, ou sistemas, inclusive conceder direitos de acesso a um usuário, a um programa, ou a um processo.

O ato de tentar entrar ou danificar um sistema, desviando-se dos seus controles de segurança. Um ataque pode buscar a obtenção de informações privilegiadas, a sua alteração ou a sua indisponibilização. O sucesso de um ataque depende da vulnerabilidade do sistema (vítima), da atividade e da eficácia de contramedidas existentes.

Ataque de Indisponibilidade (Deny of Service)

Uma rede composta por várias sub-redes. O backbone é composto por linhas de conexão de alta velocidade, que se conectam às linhas de menor velocidade.

O ataque que visa derrubar o equipamento ou aplicativo que possui algum tipo de informação, tornando-o indisponível. Alguns exemplos famosos são o "ping da morte", Winnuke e "syn flood".

Ataque interno

Ataque baseado no software ou no hardware para permitir que outras pessoas entrem no sistema e executem determinadas funções. Normalmente pode ser ativado de alguma maneira aparentemente inocente, como o acionamento de uma sequência especial de caracteres.

Um ataque originado de dentro da rede protegida, normalmente por um funcionário da organização ou alguém infiltrado na mesma.

Back-Up

Auditoria

Cópia rotineira dos dados para assegurar a sua recuperação caso sejam perdidos ou danificados.

Revisão e exame dos registros e das atividades do sistema para avaliar sobre sua confiabilidade, executados com independência.

Bastion Host

Autenticação

Ato de verificar a identidade de um usuário, de dispositivo, ou de outra entidade em um sistema computadorizado, frequentemente como um pré-requisito a permitir o acesso aos recursos em um sistema.

Authentication Token (Dispositivo de Autenticação)

Um dispositivo (equipamento) portátil usado para autenticar um usuário. O dispositivo pode operar por desafio/resposta, por seqüências de código baseado em tempo, ou por outras técnicas.

Autorização

O processo de determinar que tipos de atividades são permitidos. Geralmente, a autorização está no contexto da autenticação: uma vez que você autentica um usuário, está também autorizando acessos e/ou atividades. O poder dado pela gerência aos indivíduos específicos que permite que aprovelem transações, procedimentos, ou sistemas; inclusive conceder direitos de acesso a um usuário, a um programa, ou a um processo.

B**Backbone**

Espinha dorsal. Estrutura de nível mais alto em uma rede composta por várias sub-redes. O backbone é composto por linhas de conexão de alta velocidade, que se conectam às linhas de menor velocidade.

Back door (porta dos fundos)

Um mecanismo escondido no software ou no hardware para permitir que outras pessoas entrem no sistema e executem determinadas funções. Normalmente pode ser ativado de alguma maneira aparentemente inocente, como o acionamento de uma seqüência especial de teclas ou conexão à uma porta específica de rede.

Back-Up

Cópia rotineira dos dados para assegurar a sua recuperação caso sejam perdidos ou corrompidos.

Bastion Host

Um sistema montado para resistir a ataques que é instalado numa rede potencialmente sujeita a ataques. Bastion hosts são freqüentemente componentes de firewalls, ou podem ser servidores web externos ou sistemas de acesso público.

BBS (Bulletin Board System)

Uma base de dados, que pode ser acessada remotamente por um microcomputador e um modem utilizando a linha telefônica, onde normalmente são disponibilizados arquivos de todos os tipos, softwares de domínio público e conversas on-line (chat). Muitos BBS oferecem acesso ao correio eletrônico da Internet.

Bug

Falha (defeito) de software, que pode se comportar de forma imprevisível sobre determinadas condições. Um bug pode ser explorado intencionalmente e causar uma falha na segurança.

C

Cavalo de Tróia (Trojan horse)

Um programa de computador que contenha, escondidas, funções adicionais que exploram secretamente as autorizações do processo provocando perda da segurança. Tipo de ataque em que um software aparentemente inofensivo inicia, de forma escondida, ataques ao sistema.

Certificação de Segurança

A avaliação detalhada das características técnicas e não técnicas da segurança de um sistema e de suas proteções. Estabelece a extensão a que um projeto e/ou uma execução particulares se encontram em relação a um conjunto especificado de exigências da segurança.

Certificado Digital

Representação da chave pública de uma pessoa, entidade ou servidor específico, associando a chave ao seu proprietário, com autenticação da autoridade certificadora que o emitiu.

CERT

Computer Emergency Response Team. Organismo criado em 1988 pela Darpa, visando tratar questões de segurança em redes, em particular na Internet

Controle de acesso (Access Control)

Controle do uso de um determinado recurso garantindo a prevenindo contra o uso não autorizado. As tarefas executadas passam por mecanismos de controles que fazem a monitoração do sistema, garantindo a integridade dos dados, identificando os usuários, registrando seus acessos e as mudanças no sistema.

Cookies

Permitem que servidores gravem informações de seu interesse, geralmente de configuração, no lado cliente (browser).

Correio Eletrônico

O e-mail é um meio de comunicação baseado no envio e recepção de textos, chamados de mensagens, através de uma rede de computadores. Cada usuário de e-mail possui um endereço Internet para corresponder-se.

Cracker

(1)
Indivíduo que faz de tudo para invadir um sistema alheio, quebrando sistemas de segurança, para poder espionar ou causar danos.

Cracker

(2)
Especialista em informática que objetiva invadir ou explorar a falha de sistemas buscando o acesso, alteração ou destruição de informações privilegiadas. Tradicionalmente, o "cracker" é como chamamos o "hacker" que objetiva causar algum tipo de prejuízo à sua vítima. Pode ser motivado por razões financeiras, políticas, espionagem, etc. Veja também "Hacker".

Criptografia (Negação de Serviço)

Princípios, maneiras e métodos para esconder informações, garantindo que possam ser restauradas para uma forma inteligível. Permite disfarçar a informação de modo que não possa ser compreendida por uma pessoa desautorizada. A transformação de uma sequência de caracteres em outra por meio de uma cifra, de uma tabela de transposição, ou de um algoritmo a fim fazer com que a informação não seja entendida a qualquer um que não possua o mecanismo da decodificação.

Criptografia S ou triplo DES, em que se usa três vezes a chave de 56 bits, resultando em uma chave de 168 bits.

Criptografia é a técnica de converter (cifrar) uma mensagem ou mesmo um arquivo utilizando um código secreto. Com o propósito de segurança, as informações nele contidas não podem ser utilizadas ou lidas até serem decodificadas.

Confidencialidade Técnica de autenticação na qual um servidor emite um desafio (uma palavra, frase ou resposta desconhecido ao usuário, que retorna uma resposta usando algum dispositivo de autenticação em seu poder (programa ou token).

Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. O conceito de garantir a informação sensível confidencial, limitada para um grupo apropriado de pessoas ou organizações

Cyberspace Método de acesso a uma rede ou computador remoto via rede telefônica, discando o número de ou computador.

DNS (Domain Name System)

Por cyberspace designa-se habitualmente o conjunto de computadores, serviços, enfim toda atividade que constitui a rede Internet. Mundo virtual, onde transitam as mais diferentes formas de informação e onde as pessoas que fazem parte da sociedade da informação se relacionam virtualmente, por meios eletrônicos. Termo cunhado em analogia com o espaço sideral explorado pelos astronautas inventado por William Gibson no seu romance Neuromancer.

Domínio ou Domain Name

Doma que descreve a organização com a qual um endereço na Internet está vinculado. Faz parte da hierarquia de nomes de grupos ou hosts da Internet, identificando as instituições na rede. Exemplo: uol.com.br, onde telefônica indica a organização, com indica comercial e br indica do Brasil.

Daemon Demônio Público, (software de)

Programa em execução num computador servidor e está sempre pronto para receber solicitações de outros programas, executar determinada ação e retornar a resposta adequada.

de licenciamento para uso. Em geral, o software é utilizado sem custos por instituições educacionais, e não tem garantia de manutenção ou atualização. Um dos grandes trunfos da Internet é a quantidade praticamente inagotável de software de domínio público, com

Denial of service (Negação de Serviço)

Ataque que visa o impedimento do acesso a determinados equipamentos ou recursos ou o retardamento de operações críticas.

DES

Algoritmo de criptografia simétrico com chave de 56 bits. Existe também uma variação chamada 3DES ou triplo DES, em que se usa três vezes a chave de 56 bits, resultando em uma chave de 168 bits.

Desafio/Resposta

Técnica de autenticação na qual um servidor emite um desafio (uma palavra, frase ou sequência de caracteres) desconhecido ao usuário, que retorna uma resposta usando algum dispositivo de autenticação em seu poder (programa ou token).

Dial-Up

Método de acesso a uma rede ou computador remoto via rede telefônica, discando o número onde está a rede ou computador.

DNS (Domain Name System)

É um serviço e protocolo da família TCP/IP para o armazenamento e consulta de informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes Internet em seus números correspondentes.

Domínio ou Domain Name

Nome que descreve a organização com a qual um endereço na Internet está vinculado. Faz parte da hierarquia de nomes de grupos ou hosts da Internet, identificando as instituições na rede. Exemplo: netds.com.br, onde telefônica indica a organização, com indica comercial e br indica do Brasil.

Domínio Público, (software de)

Programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso. Em geral, o software é utilizável sem custos para fins estritamente educacionais, e não tem garantia de manutenção ou atualização. Um dos grandes trunfos da Internet é a quantidade praticamente inesgotável de software de domínio público, com

excelente qualidade, que circula pela rede.

Download (frequently Asked Questions)

O processo de se transferir uma cópia de um arquivo em um computador remoto para outro computador através da rede; o arquivo recebido é gravado em disco no computador local. O computador de onde os dados são copiados é subentendido como "maior" ou "superior" segundo algum critério hierárquico, enquanto o computador para o qual os dados são copiados é subentendido "menor" ou "inferior" na hierarquia. O sentido literal é, portanto "puxar para baixo".

(1) Um sistema ou combinação de sistemas que faz a conexão de forma segura entre duas ou mais redes. É instalado na fronteira entre elas, isolando, protegendo, monitorando e restringindo o acesso das conexões que passam por ele.

E-Mail

Firewall

Correio eletrônico.

Barreira corta fogo, em sua tradução literal. Dispositivo que controla o tráfego entre a Internet e uma rede local. Impede que usuários não autorizados entrem numa rede local, via Internet, ou que dados de um sistema saiam na Internet, sem prévia autorização.

Endereço Internet

O e-mail, é formado por usuário@domínio. Exemplo: user@telefonica.com.br. Para acesso às páginas de um site WWW utilize protocolo://www.dominio. Exemplo: http://www.telefonica.com.br.

No exemplo acima, a classificação da organização é: com (comercial), edu (educacional), gov (governo), mil (órgão militar), org (outra organização) e net (gateway ou host). O identificador de país utiliza geralmente duas letras: br (Brasil), au (Austrália), exceto para os Estados Unidos que não utiliza.

FTP anônimo

Escuta (Sniffing) (frequently Asked Questions)

Interceptação de tráfego de informação de uma maneira desautorizada com o uso de equipamentos apropriados, chamados de sniffers.

Ethernet

Um sistema distribuído para busca e recuperação de documentos, que combina recursos de navegação através de coleções de documentos e bases de dados indexadas por meio de

Um padrão muito usado para a conexão física de redes locais, originalmente desenvolvido pelo Palo Alto Research Center (PARC) da Xerox nos EUA. Descreve protocolo, cabeamento, topologia e mecanismos de transmissão. Os dados trafegam a velocidade nominal de 10 Mbps.

F

FAQ (Frequently Asked Questions)

É um arquivo contendo uma lista de perguntas mais freqüentes relativas às dúvidas mais comuns sobre determinado assunto. As respostas destas perguntas são fornecidas por usuários mais antigos, experientes ou pelo responsável por determinado serviço. As FAQ's em geral são dirigidas para leigos ou neófitos. Contrapõe-se a RFC's.

Firewall

(1)

Um sistema ou combinação de sistemas que faz a conexão de forma segura entre duas ou mais redes. É instalado na fronteira entre elas, isolando, protegendo, monitorando e restringindo o acesso das conexões que passam por ele.

Firewall

(2)

Parede corta fogo, em sua tradução literal. Dispositivo que controla o tráfego entre a Internet e um computador ligado a ela. Impede que usuários não autorizados entrem neste computador, via Internet, ou que dados de um sistema caiam na Internet, sem prévia autorização.

FTP (File Transfer Protocol)

Protocolo padrão de transferência de arquivos entre computadores, usado normalmente para transmitir ou receber arquivos via Internet.

FTP anônimo

Serviço que possibilita o acesso a repositórios públicos de arquivos via FTP

G

Gopher

Um sistema distribuído para busca e recuperação de documentos, que combina recursos de navegação através de coleções de documentos e bases de dados indexadas, por meio de menus hierárquicos. O protocolo de comunicação e o software seguem o modelo cliente-servidor, permitindo que usuários em sistemas heterogêneos naveguem, pesquisem e recuperem documentos armazenados em diferentes sistemas, de maneira simples e intuitiva.

H ML (Hypertext Markup Language)

Hacker

Linguagem padrão usada para escrever páginas de documentos para Web ou WWW. É uma variante da SGML (Standard Generalized Markup Language), bem mais fácil de aprender e

(1) Habitualmente (e erradamente) confundido com cracker. Sob uma nova óptica, mais moderna, um hacker é um expert ou Problem Solver, aquele que apresenta soluções para problemas técnicos relativos a Internet.

HTTP (HyperText Transfer Protocol)

Hacker

(2) protocolo é o conjunto de regras que permite a transferência de informações na Web e Pessoa que pesquisa sistemas a fim de descobrir falhas que o permitam invadir ou explorar algum equipamento, servidor ou aplicativo específico. Tradicionalmente, o hacker é um especialista em informática que estuda alguns equipamentos e sistemas à fundo e descobre furos nos mesmos, porém sem intenções malignas. Veja também "Cracker".

HTTPS (HyperText Transfer Protocol)

Hacking

O HTTPS é a utilização do protocolo HTTP (HyperText Transfer Protocol) em conjunto com Uma tentativa desautorizada em alcançar um sistema. Usado freqüentemente na referência a uma pessoa que tenta entrar numa base de dados de um sistema, de uma posição remota passando pela rede controla.

Home Page

Página inicial de um site da Web. Referenciado por um endereço eletrônico ou hiperlinks. É a página de apresentação da empresa ou instituição. Escrita em HTML, pode conter textos, imagens, sons, ponteiros ou links para outras páginas ou outros servidores da Internet, etc.

Host

Computador principal num ambiente de processamento distribuído. Computador central que controla uma rede. Na Internet é qualquer computador ligado à rede, não necessariamente um servidor.

Host-based Security

A condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas.

A técnica de proteger um sistema individual do ataque. Segurança baseada no host depende do sistema operacional e dos aplicativos instalados, além de necessidades específicas.

1 - Com inicial minúscula, significa a "rede das redes". Originalmente criada nos EUA, tornou-se uma associação mundial de redes interligadas, em mais de 70 países. Os computadores utilizam a arquitetura de protocolos de comunicação TCP/IP. Originalmente desenvolvida para o exército americano, hoje é utilizada em grande parte para fins

HTML (Hypertext Markup Language)

Linguagem padrão usada para escrever páginas de documentos para Web ou WWW. É uma variante da SGML (Standard Generalized Markup Language), bem mais fácil de aprender e usar, possibilitando preparar documentos com gráficos e links para outros documentos para visualização em sistemas que utilizam Web.

HTTP (HyperText Transfer Protocol)

Este protocolo é o conjunto de regras que permite a transferência de informações na Web e permite que os autores de páginas de hipertextos incluam comandos que possibilitem saltos para recursos e outros documentos disponíveis em sistemas remotos, de forma transparente para o usuário.

HTTPS (HyperText Transfer Protocol)

O HTTPS é a utilização do protocolo HTTP (HyperText Transfer Protocol) em conjunto com o protocolo SSL (Secure Sockets Layer), que é um protocolo proposto por um grupo liderado pela Netscape Communications, pela Verisign e pela Sun desenvolvido e especificado para prover uma camada de segurança entre a camada de transporte (TCP) e os protocolos de aplicação tais como HTTP, TELNET, FTP, etc. O protocolo SSL provê segurança de conexão com duas propriedades básicas:

- A conexão é privada. O mecanismo de encriptação é utilizado depois de uma negociação inicial (handshake) com a finalidade de definir uma chave secreta. Durante esta fase é utilizado a criptografia simétrica para encriptação dos dados, tal como DES ou RC4.
- A identidade do cliente e do servidor pode ser autenticada usando algoritmo de criptografia com chave assimétrica ou pública, tal como RSA ou DSS.

I

Integridade

A condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas.

Internet

1 - Com inicial maiúscula, significa a "rede das redes". Originalmente criada nos EUA, tornou-se uma associação mundial de redes interligadas, em mais de 70 países. Os computadores utilizam a arquitetura de protocolos de comunicação TCP/IP. Originalmente desenvolvida para o exército americano, hoje é utilizada em grande parte para fins

acadêmicos e comerciais. Provê transferência de arquivos, login remoto, correio eletrônico, news e outros serviços;

ISDN (Integrated Services Digital Network)

2 - Com inicial minúscula significa genericamente uma coleção de redes locais e/ou de longa distância, interligadas por pontes, roteadores e/ou gateways.

Intranet

São redes corporativas que se utilizam da tecnologia e infra-estrutura de comunicação de dados da Internet. São utilizadas na comunicação interna da própria empresa e/ou comunicação com outras empresas.

Intrusion Detection

Técnica que busca a detecção das tentativas de invasão em um sistema ou em uma rede, antes que esta tenha sucesso.

Intrusion Detection System (IDS)

Sistema automatizado de identificação de tentativas de ataques e invasões, baseado na identificação de padrões conhecidos e pré-estabelecidos.

IP (Internet Protocol)

Protocolo responsável pelo roteamento de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e usada na Internet. É o mais importante dos protocolos em que a Internet é baseada.

IP Spoofing

Uma técnica em que o atacante assume ilicitamente a personalidade de outro sistema usando seu endereço de rede IP. Objetiva enganar os dispositivos de controle, uma vez que o pacote de rede terá como endereço de origem um equipamento diferente do original, provavelmente com restrições de acesso menos rígidas.

IRC (Internet Relay Chat)

Serviço que possibilita a comunicação escrita on-line entre vários usuários pela Internet. É a forma mais próxima do que seria uma "conversa escrita" na rede.

ISDN (Integrated Services Digital Network):

Sistema telefônico digital que, mediante o uso de equipamentos especiais, permite enviar e receber voz e dados simultaneamente através de uma linha telefônica. A Rede Digital de Serviços Integrados [RDSI] integra serviços de diversas naturezas como voz, dados, imagens, etc. e deve substituir gradualmente a infra-estrutura física atual de comunicações, em que cada serviço tende a trafegar por segmentos independentes. Disponível já em vários países, inclusive o Brasil.

ISO (International Organization for Standardization)

Uma organização internacional formada por órgãos de diversos países, tais como o ANSI (americano), o BSI (inglês), o AFNOR (francês) e a ABNT (brasileira), e que estabelece padrões industriais de aceitação mundial.

ISP (Internet Service Provider)

Empresa que fornece serviços para os usuários da rede Internet. Algumas oferecem serviços de acesso discado através de ligação telefônica. Outras oferecem serviços de projetos de Web Sites (Home Pages), projetos especiais envolvendo sistemas e programação, integração de redes, etc. Algumas empresas oferecem ao usuário conexão direta pela rede interna, a conexão com o ISP é transparente para o usuário.

J

JPEG (Joint Photographic Experts Group)

Algoritmo para comprimir imagens, criado pela associação que lhe dá nome. Existe também o Motion JPEG (MPEG), usado para comprimir imagens animadas.

Java (Café)

Linguagem orientada a objetos, com sintaxe similar a C++, porém com biblioteca bastante distinta, que permite o desenvolvimento de aplicações e applets Java. Gera código intermediário (byte codes) que são interpretados em tempo de execução, o que, juntamente com a sua biblioteca, torna a linguagem multiplataforma, permitindo que seu código seja executado nas mais diversas máquinas e sistemas operacionais, sem a necessidade de adaptação.

A Sun Microsystems, que inventou a linguagem Java, desenvolveu um browser para leitura dos applets e classes, e também um console para adaptação em outros navegadores. O Netscape Navigator bem como o Microsoft Internet Explorer já possibilitam a execução de

applets Java. Mais informações no site Java da Sun Microsystems.

K **AN (Metropolitan Area Network)**

Keyword ou Palavra-Chave

Palavra usada em ferramentas de busca ou base de dados, que traz em si o significado de um assunto; através dela, é possível localizar esse assunto.

L **elocidade de tráfego de dados, equivalente a 10 milhões de bits por segundo.**

LAN (Local Area Network)

Uma rede formada por computadores localizados no mesmo espaço físico, como uma sala ou um prédio. Limitada a distâncias de até 10 km.

Linguagem Script

São linguagens de programação cujo código fonte é interpretado pelo programa em tempo execução. Por exemplo: o browser interpreta HTML, JavaScript e Vbscript.

Links ou HiperLinks

Conexão, ou seja, elementos físicos e lógicos que interligam os computadores da rede. São ponteiros ou palavras chaves destacadas em um texto, que quando "clikadas" nos levam para o assunto desejado, mesmo que esteja em outro arquivo ou servidor.

Log (ou Trilha de auditoria)

Histórico das transações dos sistemas que estão disponíveis para a avaliação a fim a provar a correção de sua execução. Permite que as falhas e quebras na segurança sejam detectáveis.

Login

O login é o nome que o usuário utiliza para acessar o servidor da rede. Para entrar na rede, você precisa digitar sua identificação (login), seguido de uma senha (password).

M (Network File System)

MAN (Metropolitan Area Network)

É o protocolo de compartilhamento de arquivos remotos desenvolvido pela Sun Microsystems. Faz parte da família de protocolos TCP/IP.

Uma rede de abrangência metropolitana.

Mbps (Megabits por segundo):

Qualquer dispositivo, inclusive Servidores e estações de trabalho, ligado a uma rede.

Velocidade de tráfego de dados, equivalente a 10 milhões de bits por segundo.

OSI (Open Systems Interconnection)

Modem

É um modelo conceitual de protocolo com sete camadas definido pela ISO, para a

Um dispositivo que adapta um computador a uma linha telefônica. Ele converte os pulsos digitais do computador para frequências de áudio (analógicas) do sistema telefônico, e converte as frequências de volta para pulsos no lado receptor. O modem também disca a linha, responde à chamada e controla a velocidade de transmissão, em bps.

N

Navegação

Dado encapsulado para transmissão na rede. Um conjunto de bits compreendendo informação de controle, endereço fonte e destino dos nós envolvidos na transmissão.

Ato de conectar-se a diferentes computadores da rede distribuídos pelo mundo, usando as facilidades providas por ferramentas como browsers Web. O navegante da rede realiza uma "viagem" virtual explorando o ciberespaço, da mesma forma que o astronauta explora o espaço sideral.

Veja Keyword.

Perímetro de Segurança

Net

O limite onde os controles de segurança devem atuar para poderem proteger os recursos. Normalmente referido à "fronteira" entre a área (rede ou subrede) a ser protegida e o meio

The Net ou Internet, a rede.

Newsgroups (Internet Group)

O plug é um programa TCP/IP usado para testar o alcance de uma rede, enviando a uma Grupo temático de discussão do netnews. uma resposta.

NFS (Network File System)

É o protocolo de compartilhamento de arquivos remotos desenvolvido pela Sun Microsystems. Faz parte da família de protocolos TCP/IP.

Nó

Qualquer dispositivo, inclusive Servidores e estações de trabalho, ligado a uma rede.

O

OSI (Open Systems Interconnection)

É um modelo conceitual de protocolo com sete camadas definido pela ISO, para a compreensão e o projeto de redes de computadores. Trata-se de uma padronização internacional para facilitar a comunicação entre computadores de diferentes fabricantes.

P

Pacote

Dado encapsulado para transmissão na rede. Um conjunto de bits compreendendo informação de controle, endereço fonte e destino dos nós envolvidos na transmissão.

Palavra-Chave ou Keyword

Veja Keyword.

Perímetro de Segurança

O limite onde os controles da segurança devem atuar para poderem proteger os recursos. Normalmente referido à "fronteira" entre a área (rede ou subrede) a ser protegida e o meio externo à mesma.

Ping (Packet Internet Group)

O ping é um programa TCP/IP usado para testar o alcance de uma rede, enviando a nós remotos uma requisição e esperando por uma resposta.

Protocolos

Um conjunto de regras padronizado que especifica o formato, a sincronização, o envio e a verificação de erros em comunicação de dados. Uma descrição formal de

Plug-Ins

Extensões do browser, fornecidas pelo fabricante do browser ou empresas parceiras que fornecem recursos adicionais de multimídia, facilitando a visualização de textos, som, vídeo, etc. e maior interação com o usuário

Política de Segurança Corporativa (Security policy)

Ver ISP

Conjunto de diretrizes, normas e procedimentos que regulam como os ativos, incluindo informação sensível, serão gerenciados, protegidos e distribuídos para os usuários de uma organização.

POP (Point-of-Presence / Post Office Protocol)

Os tipos de serviços, gerando cache das requisições mais comuns. Os proxies armazenam uma cópia de um usuário verificam se possui a informação desejada em seu cache e, caso não tenham, consultam o servidor

1. Em português Ponto-de-Presença (PP);

Public key (chave pública)

2. Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em Servidores de correio eletrônico.

Uma chave criptográfica disponível para distribuição sem necessidade de sigilo. É o oposto

Porta

chave privada ou chave secreta

R

Uma abstração usada pela Internet para distinguir entre conexões simultâneas múltiplas para um único host destino. O termo também é usado para denominar um canal físico de entrada e saída de um dispositivo.

RFC - Acrônimo para Request For Comments. RFCs constituem uma série de documentos de 1969 a que descrevem aspectos relacionados com a Internet, como padrões, protocolos, serviços, recomendações operacionais, etc. Uma RFC é, em geral, muito densa do ponto de vista técnico

Postmaster

E-Mail do responsável pelo correio eletrônico de uma máquina ou domínio.

Protocolos

PPP (Point-to-Point Protocol)

Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede

Um dos protocolos mais conhecidos para acesso via interface serial. O PPP estabelece um método de acesso a Internet em que um computador, ligado a um host Internet via telefone e um modem de alta velocidade, aparece para o host como se fosse uma porta Ethernet no sistema de rede local do host. É considerado o sucessor do SLIP por ser confiável e mais eficiente.

Protocolo

Um conjunto de regras padronizado que especifica o formato, a sincronização, o seqüenciamento e a verificação de erros em comunicação de dados. Uma descrição formal de formatos de mensagem e das regras que dois computadores devem obedecer ao trocar mensagens. O protocolo básico utilizado na Internet é o TCP/IP.

Provedor de Acesso

Ver ISP.

Proxy

Software que concentra as conexões de alguns tipos de serviços, gerando cache das requisições mais comuns. Os proxies aceitam uma conexão de um usuário, verificam se possui a informação desejada em seu cache e, caso não possuam, consultam o servidor externo. Caso contrário, retornam a informação, sem a necessidade de fazer consulta externa.

Public key (chave pública)

Uma chave criptográfica disponível para distribuição sem necessidade de segredo. É o oposto de uma chave privada ou chave secreta.

R

RFC - Acrônimo para Request For Comments. RFCs constituem uma série de documentos editados desde 1969 e que descrevem aspectos relacionados com a Internet, como padrões, protocolos, serviços, recomendações operacionais, etc. Uma RFC é, em geral, muito densa do ponto de vista técnico.

Roteador

Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes. Uma instituição, ao se conectar à Internet, deverá adquirir um roteador para conectar sua Rede Local (LAN) ao Ponto-de-Presença mais próximo. Roteadores vivem se falando aos pares, como modems.

S

Screening Router

Um router configurado para permitir ou negar o tráfego baseado em um jogo de regras de permissão (filtro de pacotes) instaladas pelo administrador. Permite um nível básico de segurança.

Secure Hash Algorithm

Algoritmo que cria a partir da mensagem original, uma assinatura digital que garante a autenticidade da mensagem.

Security Officer

Pessoa(s) que garante(m) que os procedimentos de segurança estão de acordo com a política de segurança corporativa.

Security requirements baseline

Descrição dos requerimentos mínimos necessários para um sistema manter um nível aceitável de segurança.

Segurança da Informação

Proteção de informações para que sejam mantidos os aspectos de confidencialidade, integridade e disponibilidade.

Segurança de Perímetro (Perimeter-based Security)

Técnica de proteção de uma rede em que são monitorados e controlados os acessos em todos os pontos de entrada e saída da mesma, incluindo a conexão com a Internet, links com parceiros ou escritórios remotos, etc.

Segurança Física

Equipamentos e medidas usadas para garantir a proteção física dos recursos de informática contra ameaças voluntárias e involuntárias, como incêndio, invasões, acidentes, etc.

S

Screening Router

Um router configurado para permitir ou negar o tráfego baseado em um jogo de regras de permissão (filtro de pacotes) instaladas pelo administrador. Permite um nível básico de segurança.

Secure Hash Algorithm

Algoritmo que cria a partir da mensagem original, uma assinatura digital que garante a autenticidade da mensagem.

Security Officer

Pessoa(s) que garante(m) que os procedimentos de segurança estão de acordo com a política de segurança corporativa.

Security requirements baseline

Descrição dos requerimentos mínimos necessários para um sistema manter um nível aceitável de segurança.

Segurança da Informação

Proteção de informações para que sejam mantidos os aspectos de confidencialidade, integridade e disponibilidade.

Segurança de Perímetro (Perimeter-based Security)

Técnica de proteção de uma rede em que são monitorados e controlados os acessos em todos os pontos de entrada e saída da mesma, incluindo a conexão com a Internet, links com parceiros ou escritórios remotos, etc.

Segurança Física

Equipamentos e medidas usadas para garantir a proteção física dos recursos de informática contra ameaças voluntárias e involuntárias, como incêndio, invasões, acidentes, etc.

Servidor

Numa rede, é um computador que administra e fornece programas e informações para os outros computadores conectados. No modelo cliente-servidor, é o programa responsável pelo atendimento a determinado serviço solicitado por um cliente. Serviços como archie, Gopher, WAIS e WWW são providos por servidores; Referindo-se a equipamento, o Servidor é um sistema que prove recursos tais como armazenamento de dados, impressão e acesso dial-up para usuários de uma rede de computadores.

Shareware

Programa disponível publicamente para avaliação e uso experimental, mas cujo uso em regime pressupõe que o usuário pagará uma licença ao autor. Note-se que shareware é distinto de freeware, no sentido de que um software em shareware é comercial, embora em termos e preços diferenciados em relação a um produto comercial "ortodoxo". Veja também: freeware ou domínio público.

Site (Instalação)

Uma instituição, onde computadores são instalados e operados; No mundo virtual, é um endereço cuja porta de entrada é sempre sua home page.

SLIP (Serial Line Internet Protocol)

Serial Line IP é um protocolo serial assíncrono, bastante popular, usado na Internet para acesso remoto discado.

SMTP (Simple Mail Transfer Protocol)

Protocolo Internet usado para correio eletrônico.

SNMP (Simple Network Management Protocol)

Protocolo usado para monitorar e controlar serviços e dispositivos de uma rede TCP/IP. É o padrão adotado pela RNP para a gerência de sua rede.

Sockets

Conectores utilizados entre as aplicações e rede.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Spoofing

Família de protocolos que torna possível a comunicação de computadores de redes diferentes.

Tentativa de ganhar acesso ao sistema fazendo-se passar por um outro micro ou usuário, que normalmente seria autorizado.

Telnet

SSH (Secure Shell)

Uma das aplicações da Internet, que permite o login remoto, tornando possível a um

Programa que permite a conexão criptografada para seções de telnet e rlogin, principalmente. Pode ser extendida para outros serviços.

SSL (Secure Socket Layer)

Teste de Invasão (Penetration test)

É um padrão de comunicação, utilizado para permitir a transferência segura de informações através

O protocolo SSL provê segurança de conexão com duas propriedades básicas:

- A conexão é privada. O mecanismo de encriptação é utilizado depois de uma negociação inicial (handshake) com a finalidade de definir uma chave secreta. Durante esta fase é utilizado a criptografia simétrica para encriptação dos dados, tal como DES ou RC4.
- A identidade do cliente e do servidor pode ser autenticada usando algoritmo de criptografia com chave assimétrica ou pública, tal como RSA ou DSS.

SSL (Secure Sockets Layer)

Protocolo que possibilita realizar comunicações seguras através de criptografia e autenticação da comunicação. Utilizado para criptografar conexões HTTP.

SYSOP (SYStems OPerator)

Sistema para compartilhamento de arquivos, que permite que vários usuários compartilhem os recursos de um computador simultaneamente. Muito usado na Internet.

A pessoa responsável pela manutenção e operação de um BBS ou provedor de acesso à Internet.

Código para localização universal, que permite identificar e acessar um serviço na rede WEB. Por exemplo, a URL <http://www.telefonica.com.br> aponta para o WWW da Telefônica.

Usenet ou Usenet News

Uma coleção de newsgroups organizada por tópicos. Também é o nome de uma rede de computadores, sendo que nem todos eles estão ligados à Internet.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Vírus

Família de protocolos que torna possível a comunicação de computadores de redes diferentes. É um padrão de fato para inter-redes abertas e a linguagem universal da Internet.

Uma classe de software malicioso que tem a habilidade de se auto-replicar e infectar partes de uma operacional ou dos programas de aplicação, normalmente com o intuito de causar a perda ou dano nos dados.

Telnet

Uma das aplicações da Internet, que permite o login remoto, tornando possível a um microcomputador atuar como terminal de computadores de qualquer parte do mundo. O Telnet atua no modo texto e permite usar um computador, que está longe, como se fosse o seu próprio micro.

de segurança que permite interligar várias redes e usuários remotos através de um meio público (como a Internet), de forma que toda a comunicação seja criptografada.

Teste de Invasão (Penetration test)

Vulnerabilidade

Teste de segurança em que é avaliada a possibilidade de se conseguir a entrada não autorizada em um sistema.

associada a um equipamento (hardware, sistema operacional ou aplicativo) que pode ser explorada para causar dano ou invasão ao mesmo.

Transferência de Arquivos

FTP

Cópia de arquivos entre duas máquinas via rede. Na Internet, implantada e conhecida por FTP.

U

da rede que interliga computadores distribuídos em áreas geograficamente separadas, ou seja, um conjunto de redes locais interligadas por meios de comunicação remotos (Modem, cabos dedicados, rádio, ...)

UNIX

Wav

Sistema operacional avançado, que permite que vários usuários compartilhem os recursos de um computador simultaneamente. Muito usado na Internet.

tipo de formato de arquivo de som do Windows.

URL (Uniform Resource Locator)

WORM (Write Once Read Many)

Código para localização universal, que permite identificar e acessar um serviço na rede WEB. Por exemplo, a URL abaixo aponta para o WWW da Telefônica : <http://www.telefonica.com.br>

Usenet ou Usenet News

Uma coleção de newsgroups organizada por tópicos. Também é o nome de uma rede de computadores, sendo que nem todos eles estão ligados à Internet.

V**Vírus**

Uma classe do software malicioso que tem a habilidade de se auto-replicar e infectar partes do sistema operacional ou dos programas de aplicação, normalmente com o intuito de causar a perda ou dano nos dados.

VPN (Virtual Private Network)

Infra-estrutura de segurança que permite interligar várias redes e usuários remotos através de um meio público (como a Internet), de forma que toda a comunicação seja criptografada.

Vulnerabilidade

Bug (falha) normalmente associada a um equipamento (hardware, sistema operacional ou aplicativo) que pode ser explorada para causar dano ou invasão ao mesmo.

W**WAN (Wide Area Network) [Rede de longa distância]**

Toda rede que interliga computadores distribuídos em áreas geograficamente separadas, ou seja, um conjunto de redes locais interligadas por meios de comunicação remotos (Modems, linhas dedicadas, rádios, ...)

Wav

Tipo de formato de arquivo de som do Windows.

WORM (Write Once Read Many)

1. Ferramenta de busca na rede Web;

2. Verme, programa que, explorando deficiências de segurança de hosts, logrou propagar-se de forma autônoma na Internet na década de 80.

WWW (World Wide Web ou Web ou W3)

Literalmente, teia de alcance mundial. Baseada em hipertextos, integra diversos serviços Internet que oferecem acesso, através de hiperlinks, a recursos multimídia da Internet. Responsável pela popularização da rede, que agora pode ser acessada através de interfaces gráficas de uso intuitivo, como o Netscape ou Mosaic, a Web possibilita uma navegação mais fácil pela Internet.

MODULO SECURITY - www.modulosecurity.com.br

RFC 2328 - Request for Comments - Internet Security Glossary

SAN FRANCISCO STATE UNIVERSITY Computing & Communications Services Security Guide, 1991. Disponível em www.sfsu.edu.

SIMSON, G, Spafford G; Comércio & Segurança na Web, São Paulo, Market Press, 1999.

STARLIN, Gorko. Segurança na Internet. Rio de Janeiro: Book Express, 1999.

REFERÊNCIAS BIBLIOGRÁFICAS

CARUSO, C.; A.; A.; STEFFEN, F.; D. Segurança em Informática e de Informações 2. Ed. São Paulo: Senac. 1999.

CERT - Computer Emergency Respose Team - <http://www.cert.org>

CHIN, S. K. High-confidence design for security. Communications of the ACM, v. 42, n. 37, p. 33-37, 1999.

JÚNIOR, Teixeira; MOURA, Suave; TEIXEIRA, Ramos. Redes de Computadores – Serviços, Administração e Segurança. São Paulo: Makron Bookd, 1999.

McCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hackers Expostos. São Paulo: MakronBooks, 2000.

MÓDULO SECURITY – www.modulosecurity.com.br

RFC 2828 - Request for Coments - Internet Security Glossary

SAN FRANCISCO STATE UNIVERSITY. Computing & Communications Services Security Guide, 1991. Disponível em www.sfu.edu.

SIMSON, G, Spafford G; Comércio & Segurança na Web, São Paulo; Market Press, 1999.

STARLIN, Gorki. Segurança na internet. Rio de Janeiro: Book Express, 1999.

ICSA - Internet Consortium Security Agency - <http://www.icm.net>

Infoexame. Sites de comércio eletrônico têm falhas [on-line] <<http://www2.uol.com.br/info/infonews/031999/10031999-0.shtml>> Acesso em: 10 agosto. 2002.

JÚNIOR, Teixeira; MOURA, Suave; TEIXEIRA, Ramos. Redes de Computadores – Serviços, Administração e Segurança. São Paulo: Makron Bookd, 1999.

LYNCH, Daniel; LUNDQUIST, Leslie. Dinheiro Digital O Comércio na Internet. Rio de Janeiro: Campus, 1996.

LIENTZ, Bennet; REA, Kathryn. Comece bem no e-business. São Paulo: Market Books, 2001.

MANDIA, Kevin; PROSISE, Chris. Hackers Resposta à Contra-ataque. Rio de Janeiro: Campus, 2001.

NAKAMURA, Rodolfo. e-commerce na Internet. São Paulo: Érica, 2001.

BIBLIOGRAFIA

BARBOSA, Alexandre. Desafio: gerenciar negócios na internet. Internet Business, Rio de Janeiro, n48, p.44-46, ago.2001.

BASTOS, Alberto. Segurança da Informação na Internet e Intranet. Developer's Magazine. SãoPaulo, fevereiro/1998

BERNSTEIN, Terry; BHIMANI, Anish B. Segurança na Internet. Tradução do original Internet Security for business. 1997. Campus: Rio de Janeiro, RJ.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. Segurança em Informática e de Informações. São Paulo: Editora SENAC, 1999.

CARVALHO, Daniel Balparda de. Segurança de dados com criptografia. Rio de Janeiro: BookExpress, 2000.

E-BUSINESS - De volta aos negócios: desenvolvendo uma nova forma de pensar. Disponível em: <<http://www.br.ibm.com/e-business/portugues>>. Acesso em: 06 Junho. 2002.

GOMES, O., J., A. Segurança Total protegendo-se contra os hackers, São Paulo: Makron Books, 2000.

GONÇALVES, Marcus. Segurança na Internet: Protegendo seu Web com Firewalls. 1997. Campus: Rio de Janeiro. Rj.

HAGEL III, Hagel, ARMSTRONG, Arthur. Vantagem Competitiva na Internet. Rio de Janeiro: Campus, 1998.

ICSA - Internet Consortium Security Agency - <http://www.icsa.net>

Infoexame. Sites de comércio eletrônico têm falhas [on-line] <<http://www2.uol.com.br/info/infonews/031999/10031999-0.shl>> Acesso em: 10 agosto. 2002.

JÚNIOR, Teixeira; MOURA, Suave; TEIXEIRA, Ramos. Redes de Computadores – Serviços, Administração e Segurança. São Paulo: Makron Bookd, 1999.

LYNCH, Daniel, LUNDQUIST, Leslie. Dinheiro Digital O Comércio na Internet. Rio de Janeiro: Campus, 1996.

LIENTZ, Bennet, REA, Kathryn. Comece bem no e-business. São Paulo: Market Books, 2001.

MANDIA, Kevin; PROSISE, Chris. Hackers Resposta e Contra-ataque. Rio de Janeiro: Campus, 2001.

NAKAMURA, Rodolfo. e – commerce na Internet. São Paulo: Èrica, 2001.

NEGROPONTE, N. A vida digital. 2 a ed. Tradução de Sérgio Tellaroli. São Paulo: Companhia das Letras, 1995.

PENTEADO, S. De olho na segurança. InformationWeek. n ° 6, julho/1999, pag. 26-34.

RÔÇAS, C. Credibilidade em cheque. Internet Business. n ° 32, Abril 2000, pag. 48-55.

SANTOS, J.; Todo Cuidado é pouco; Internet Business n o 14; Outubro 1998, pg 43-45.

SARAIVA, J. Privacidade - protegendo o usuário. meiodigital. n.º 1, Maio 2000, pág. 46

SECURITY FOCUS – <http://www.securityfocus.com>

SIMSON G, Spafford G; Comércio & Segurança na Web, São Paulo; Market Press, 1999.

STARLIN, Gorki; NOVO, Rafael. Segurança na Internet. Rio de Janeiro: Book Express, 1998.

TANENBAUM, Andrew S. Redes de Computadores. Tradução do original Computer Network. 3 ed. 1994. Campus: Rio de Janeiro, RJ.

VASCONCELOS, Márcio José Accioli de. Pânico na internet. São Paulo: Chantal, 1999.