UNIVERSIDADE ANAHANGUERA

DOUGLAS DA SILVA SALVINO

SEGURANÇA DE REDES

SEGURANÇA DE REDE NO AMBIENTE CORPORATIVO

São Paulo

2017

DOUGLAS DA SILVA SALVINO

SEGURANÇA DE REDE

SEGURANÇA DE REDE NO AMBIENTE CORPORATIVO

Trabalho de Conclusão de Curso apresentado à Universidade Anhanguera como requisito parcial para a obtenção do título de graduado em Sistema de Informação.

Orientador: Mariana Nunes

São Paulo
2017

DOUGLAS DA SILVA SALVINO

SEGURANÇA DE REDE

SEGURANÇA DE REDE NO AMBIENTE CORPORATIVO

Trabalho de Conclusão de Curso apresentado à Universidade Anhanguera como requisito parcial para a obtenção do título de graduado em Sistema de Informação.

BANCA EXAMINADORA

Prof(º). MAURICIO FAZOLI

Prof(ª). LUCIANA APARECIDA MAXIMIAMO

Prof(ª). CLEYTON FERREIRA FRANCO

São Paulo, 19 de novembro de 2017.

SALVINO, Douglas Silva. **Segurança de rede**: Segurança de rede no ambiente corporativo. 2017. 39. Trabalho de Conclusão de Curso (Graduação em Sistema de Informação) – Universidade Anhanguera, São Paulo, 2017.

RESUMO

Este trabalho busca mostrar a partir de uma pesquisa bibliográfica, os principais métodos utilizados por organizações corporativas na hora de proteger seus arquivos e informações confidenciais compartilhados em redes internas ou externas, de modo que apenas pessoas autorizadas tenham acesso aos mesmos. Sendo assim, este estudo irá caracterizar modos de proteger as redes de Spam, phishing e vírus que possam atingir seus computadores. Serão estudados métodos seguros para uma organização proteger suas informações contra quaisquer ataques e falhas que possam atingi-las. Serão abordados programas mal intencionados que podem atingir os computadores e sistemas que podem ajudar a se proteger e resolver os problemas causados por tais programas maldosos.

Palavras-chave: Proteger; Confidenciais; Organizações; redes; Computadores.

SALVINO, Douglas Silva. **Segurança de rede**: Segurança de rede no ambiente corporativo. 2017. 39. Trabalho de Conclusão de Curso (Graduação em Sistema de Informação) – Universidade Anhanguera, São Paulo, 2017.

ABSTRACT

This work searchs to show from a bibliographical research, the main methods used for corporative organizations in the hour to protect its shared archives and confidential information in internal or external nets, in way that only authorized people have access to the same ones. Being thus, this study it will go to characterize ways to protect the nets of Spam, phishing and viruses that can reach its computers. Safe methods will be studied an organization to protect its information against any attacks and imperfections that can atingiz them. They will be boarded badly intentioned programs that can reach the computers and systems that can help if protect and decide the problems caused for such malicious programs.

***Key-words*: To protect; Confidential; Organizations; nets; Computers.**

LISTA DE ILUSTRAÇÕES

Figura 3.1 – Funcionamento do Firewall 17
Figura 3.2 – Tipos de Firewall e como se aplicam 20
Figura 4.1 – Tipos de Ataques 25
Figura 5.1 – Fases do vírus biológicos 29

SUMÁRIO **7**

1. INTRODUÇÃO **9**

2. INTRODUÇÃO A SEGURANÇA DE REDE **10**

2.1. FUNDAMENTOS DE SEGURANÇA DE COMPUTADORES 10

2.2. CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE. 11

2.2.1. Confidencialidade 12

2.2.2. Integridade 12

2.2.3. Disponibilidade 13

2.3. CONCEITOS DE REDES 13

2.3.1. Topologia de Redes. 14

2.4. O AMBIENTE CORPORATIVO. 14

2.4.1. Problemas no ambiente corporativo. 15

3. Firewalls **17**

3.1. CARACTERÍSTICAS DO FIREWALL 18

3.2. FUNCIONALIDADES 18

3.2.1. Filtros 18

3.2.2. Proxies 19

3.2.3. Bastion hosts 19

3.2.4. Zona desmilitarizada 19

3.3. TIPOS DE FIREWALL 19

3.4. SISTEMAS CONFIÁVEIS DE FIREWALL 21

4. Criptografia **22**

4.1.1. Encriptação 22

4.1.2. Criptossistemas 22

4.1.3. Encriptação simétrica 23

4.2. CIFRAS TRADICIONAIS 23

4.2.1. Cifra de Substituição 23
4.2.2. Cifras de Transposição.....24
4.3. ATAQUES 24
5. PROGRAMAS MALICIOSOS (MALWARE) 27
5.1. DEFESAS CONTRA ATAQUES INTERNOS. 27
5.2. VÍRUS DE COMPUTADOR 28
5.2.1. Classificação de vírus. 29
5.2.2. Tipos de Vírus. 30
5.3. DEFESAS CONTRA VÍRUS. 30
5.3.1. Vírus encriptados.....31
5.4. BOAS PRÁTICAS. 31
5.4.1. Boas praticas adicionais. 32
6. POLÍTICA DE SEGURANÇA 33
6.1. O PLANEJAMENTO. 33
6.2. OS ELEMENTOS. 34
6.3. A IMPLEMENTAÇÃO. 35
6.4. POLITICA DE SEGURANÇA NO AMBIENTE CORPORATIVO. 36
7. CONSIDERAÇÕES FINAIS 38
8. REFERÊNCIAS 39

1. INTRODUÇÃO

Em 2017, é possível observar que o número de microempresas cresceu de maneira significativa, e o conceito de segurança de redes está mais requisitado. As empresas utilizam arquivos compartilhados em servidores, para acesso de clientes e dos próprios funcionários, com isso se preocupam em ter métodos seguros de proporcionar acesso às informações sem que a integridade dos documentos seja comprometida.

Muitas organizações se deparam com falhas em seus sistemas de segurança. Tendo prejuízos financeiros desnecessários e até perda de clientes. Para proteger seus computadores de vírus, hackers, perda de dados, e outros problemas, é necessário conhecer métodos de segurança de redes.

O uso indevido dos dados e dos recursos de web disponíveis sem nenhuma política de segurança deixa os dados vulneráveis. Sendo assim como é possível assegurar que as empresas guardem suas informações, arquivos e principalmente dados confidenciais, utilizando rede interna ou externa, sem que os documentos possam ser divulgados ou alterados?

Este estudo busca estudar conceitos de redes e de segurança no ambiente corporativo, caracterizando modos de proteger os arquivos contra quaisquer perigos que possam atingi-los. Apresentar modelos de regras de Firewall, criptografia e antivírus, e políticas de bloqueio de segurança, descrever formas seguras de verificação dos equipamentos de rede, pesquisar procedimentos de segurança para que as aplicações de web não contenham vírus e também não permitam acesso indevido aos servidores da rede por Hackers.

O estudo foi feito através de uma pesquisa bibliográfica realizada na internet, em arquivos científicos, e em livros. Foi realizada uma pesquisa exploratória, e a análise dos dados foi qualitativa, pois foram estudados alguns métodos de segurança de rede, para proteger os arquivos confidenciais compartilhados através de uma rede. Após análise e avaliação dos dados coletados, foi apresentado o método mais seguro de proteger os arquivos de organizações coorporativas contra-ataques e falhas que podem atingir seus documentos compartilhados em redes.

2. INTRODUÇÃO A SEGURANÇA DE REDE

Nakamura E Lício (2007), no livro Segurança de Redes em ambiente cooperativo, afirmam que a informática e as telecomunicações vêm se tornando cada vez mais essenciais para o sucesso das organizações, nesse cenário se dá o surgimento do ambiente corporativo. A partir daí novos problemas aparecem em especial a relação à segurança de dados e arquivos.

A internet está cada vez mais presente na vida das pessoas e nas organizações, é indispensável para uma empresa o acesso à internet. Porém, o uso da internet acaba por deixar os sistemas das organizações mais vulneráveis, sendo assim, é necessário o uso de métodos de firewalls, Políticas de Segurança e a separação entre rede interna e externa.

Nakamura e Lício (2007) afirmam também que a internet facilita e aumenta a velocidade em vários processos dentro das organizações, mas em contrapartida essa facilidade pode resultar em prejuízos e grandes problemas para os negócios. Dificilmente uma empresa se mantém livre de invasões, já que existe uma contínua evolução de ataques, que necessitam que os métodos de segurança também avancem.

2.1. FUNDAMENTOS DE SEGURANÇA DE COMPUTADORES

De acordo com Nakamura e Lício (2007), “existe uma a cada vez maior dependência da informática e das telecomunicações por parte das organizações, o que faz com que um novo ambiente de extrema importância surja no ambiente computacional: ambiente corporativo”.

Tanebaum (2003) no livro *Computer Networks* afirma que as redes têm a função de compartilhar recursos, e o objetivo de tornar todos os programas, equipamentos e dados ao alcance de todas as pessoas na rede, independente de sua localização. Porém, com o passar do tempo às redes foram adquirindo milhares de novas funções e a partir daí os problemas com essa expansão também se tornaram mais frequentes, com o uso desenfreado e não calculado, dados sigilosos passaram a trafegar pela rede. E nenhum programa criado produz segurança perfeita, é necessário assegurar que um programa de proteção seja realmente eficaz, e quando uma falha ocorrer ter planos adequados para atendê-las.

Conforme Goodrich, e Tamassia (2013) dizem no livro “Introdução à Segurança de Computadores”, para manter a segurança de computadores no ambiente corporativo é necessário encontrar as vulnerabilidades dos sistemas de computadores que permitem o acesso de usuários não permitidos a dados confidenciais ou até mesmo à invasão e controle da máquina. Podem ocorrer diversos tipos de ataques de acordo com o grau de vulnerabilidade da máquina. Quando ocorre um ataque é necessário identificar as máquinas comprometidas, remover o dano implantado e corrigir as vulnerabilidades do sistema.

Goodrich, e Tamassia (2013) dizem também que os Modelos sólidos são o ponto de partida para se adquirir um sistema de computador seguro, e em seguida definir as propriedades de segurança que precisam ser protegidas, prevendo ataques à que o sistema possa ser submetido e criando defesas específicas. O projeto de segurança deve levar em consideração a forma que será posta em prática, já que um projeto difícil de entender e seguir dificilmente obterá sucesso. Após a criação do projeto e a implementação de tal, diversos testes devem ser executados a fim de identificar erros que podem causar vulnerabilidade. Com a finalização do sistema, é preciso monitorar e estar atento a falhas de segurança que podem ser detectadas para assim efetuar as correções necessárias.

2.2. CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE.

A invasão de uma máquina ou sistema pode causar um prejuízo financeiro sério a organizações, portanto, existe uma grande necessidade de segurança por parte de tais.

Goodrich e Tamassia (2013), falam que, “tradicionalmente, segurança da informação tem sido definida nos termos do acrônimo C.I.D. (do inglês C.I.A., *confidentiality, integrity, availability*), que significam confidencialidade, integridade e disponibilidade. E descrevem que a confidencialidade é evitar a revelação não autorizada de informação, a integridade é a propriedade de que a informação não foi alterada de maneira não autorizada e a disponibilidade é a propriedade da informação ser acessível e modificável no momento oportuno por aqueles que estejam autorizados a fazer isso”.

2.2.1. Confidencialidade

A confidencialidade na segurança do computador permite a proteção de dados sigilosos, de forma que somente pessoas autorizadas tenham acesso aos mesmos.

Segundo Goodrich e Tamassia (2013), para alcançar a confidencialidade, diversos sistemas foram criados e algumas das ferramentas utilizadas são:

- Encriptação que é a proteção de uma informação usando um código chamado de chave de encriptação, e só se obtém acesso a tal informação através desse código.
- Controle de acesso que é a limitação de algumas informações para apenas algumas pessoas ou sistemas, através do nome ou série da máquina.
- Autenticação que é a determinação da identidade ou papel de alguém através de senha, impressão digital, entre outras maneiras.
- Autorização através de uma política de controle de acesso que determina se o usuário tem ou não acesso às informações.

Goodrich e Tamassia (2013) afirmam “Que manter a informação secreta é muitas vezes a essência da segurança de informação, e esse conceito, na verdade, antecede os computadores”.

2.2.2. Integridade.

A Integridade é a certeza de que as informações não foram alteradas por pessoas não autorizadas, mantendo a confidencialidade segura. Segundo Goodrich e Tamassia (2013), a integridade dos dados pode ser comprometida de maneira benigna como uma interferência decorrente de uma radiação ou um disco que estraga, ou de modo malicioso como um vírus que infecta o sistema e os arquivos. Algumas ferramentas foram criadas para o auxílio da integridade dos computadores, sendo elas:

- Cópias de segurança de modo que as informações sejam salvas periodicamente, fazendo com que se algum arquivo for alterado, tenha a possibilidade de recuperar o modelo salvo anteriormente.
- soma de verificação que mapeiam o conteúdo de forma numérica, sendo assim se ocorrer alguma modificação será perceptível por resultar em um valor de saída diferente.

- Código de correção de dados que permite que pequenas alterações sejam percebidas e alteradas automaticamente.

Essas ferramentas auxiliam as empresas no processo de manter a integridade dos computadores.

2.2.3. Disponibilidade

A disponibilidade é terceira parte fundamental da segurança da informação, Goodrich e Tamassia (2013), afirmam que a disponibilidade é a propriedade que permite o acesso e modificação de arquivos em determinado momento e por pessoas autorizadas. Foram criadas também ferramentas que mantenham a disponibilidade dos computadores, como:

- Proteções físicas que são uma infraestrutura planejada que proteja as informações mesmo enfrentando problemas, como por exemplo, equipamentos que mantenham o computador ligado mesmo em quedas e picos de energia.
- Redundâncias computacionais que são dispositivos ou máquinas de armazenamento reservam utilizadas em caso de falhas.

Sendo assim, as proteções físicas e as redundâncias computacionais são ferramentas que mantém a disponibilidade dos computadores.

2.3. CONCEITOS DE REDES.

Durante as guerras, os militares utilizavam meios de se comunicar, porém as informações extraviavam para o inimigo tornando-os vulneráveis, sendo assim surgiu a Internet com uma comunicação segura, evitando ataques militares. Tendo em vista que a Internet surgiu para esse propósito, foi determinado um modo de proteger as informações contendo um pacote de dados que é muito utilizado para a comunicação de terceiros.

Como dizem Googrich e Tamassia (2013), “se duas entidades desejam se comunicarem através da Internet, elas precisam mandar suas mensagens em pacotes, anexando um cabeçalho em cada um e depois deixar que os pacotes encontrem o seu caminho na Internet para chegar até seu destino”.

Afirmam também que um pacote de Dados nada mais é do que uma junção de Bits, que é separada em:

- Cabeçalho: que identifica o caminho do pacote e carrega consigo detalhes de sobrecarga e de administração.

• Carga: que é o pacote de dados sendo enviado como uma informação.

2.3.1. Topologia de Redes.

A estrutura de conexão de uma rede recebe o nome de Topologia de Rede. As redes computacionais são conhecidas como nodos host, e são origem ou destino de informações e os roteadores são denominados nodos de comunicação, e são os meios pelos quais as mensagens são enviadas ou recebidas. Os nodos em uma conexão física possuem uma forma de estabelecer canais que viajam passando de nodo a nodo saindo da origem e chegando a seu destino.

Forouzan (2010) no Livro A Comunicação de dados e Redes de Computadores, afirma que a comunicação na rede é host-host, que significa computador – computador. E um computador que precisa se comunicar com outro computador normalmente se comunica pela Internet. O pacote transmitido pelo computador transmissor passa por várias LANs ou WANs até atingir o computador de destino.

De acordo com Goodrich e Tamassia (2013), uma rede privada com diversas unidades de computadores que possuem uma a proximidade é conhecida como uma rede de área local ou também como LAN, e a Internet é chamada rede de área ampla, ou WAN, composta por diversas máquinas e redes espalhadas a grandes distâncias. Dentre as redes de área ampla, existem os sistemas Autônomos (Sas) que são roteadores de ampla conexão com a Internet separada em grupos. E cada sistema autônimo possui um controle único em sua organização, que é decretará como funcionará o pacote que será roteado para os nodos desse sistema.

Goodrich e Tamassia (2013) dizem que normalmente, esses roteadores que fazem parte de um sistema autônimo se utilizam a trilha mais curta, de forma a diminuir os pulos de nodo a nodo dentro do SA (sistema autônimo), barrando assim os ciclos de roteamento. O roteamento entre sistemas autônimos é estabelecido por modelos de acordos contratuais, mas visa evitar laços entre os mesmos.

2.4. O AMBIENTE CORPORATIVO.

Nakamura e Lício (2007) citam que com o mundo globalizado, as organizações passaram a competir cada vez mais pelas novas formas de mercado. É cada vez mais fácil, através das tecnologias digitais, competir com organizações que podem estar localizadas até do outro lado do planeta. Portanto, é necessário

manter o nível dos serviços prestados no mais alto padrão. E manter relações comerciais cada vez mais fortes.

Nakamura e Lício (2007) afirmam também que no século XXI, a competitividade entre as organizações é ditada pela velocidade e qualidade das implementações e das comunicações. Sendo assim, é essencial uma boa infraestrutura de telecomunicações para que a comunicação das organizações e recursos seja eficiente. O uso das tecnologias de maneira eficiente pode resultar na evolução dos negócios e no surgimento de novas oportunidades. Portanto, as tecnologias digitais se tornaram vitais para a sobrevivência das organizações.

2.4.1. Problemas no ambiente corporativo.

De acordo com Nakamura e Lício (2007), um dos problemas que acomete o ambiente corporativo é a dificuldade de comunicação entre os diferentes tipos de organizações, cada uma com suas características. Porém, a junção de protocolos de TCP/IP e a internet facilitam a comunicação entre as organizações de forma mais simples e barata. Entretanto, esse feito tem impactos negativos na proteção das particularidades de cada organização.

Um desses impactos é o acesso não autorizado de pessoas ou organizações a informações confidenciais que são compartilhadas em redes. Nakamura e Lício (2007) usam como exemplo uma organização que disponibiliza o acesso à informação a uma segunda organização, mas não para uma terceira, que, no entanto, consegue acesso a tais informações através dessa segunda com a qual mantém contato, prejudicando assim a confidencialidade, integridade e a disponibilidade das informações da organização primária.

Nakamura, e Lício (2007), falam que, “a necessidade cada vez maior de conexões resulta em uma complexidade nas configurações de redes de todos os envolvidos. Com isso, é formado um ambiente corporativo que traz consigo uma série de implicações de segurança, principalmente quanto aos limites entre as redes e aos perigos de triangulações”.

Para se obter segurança em ambientes corporativos, é necessário compreender o ambiente e as tecnologias de modo a utilizá-las corretamente. Tendo em vista diversas técnicas de segurança, fica difícil escolher a técnica mais adequada para proteger uma rede.

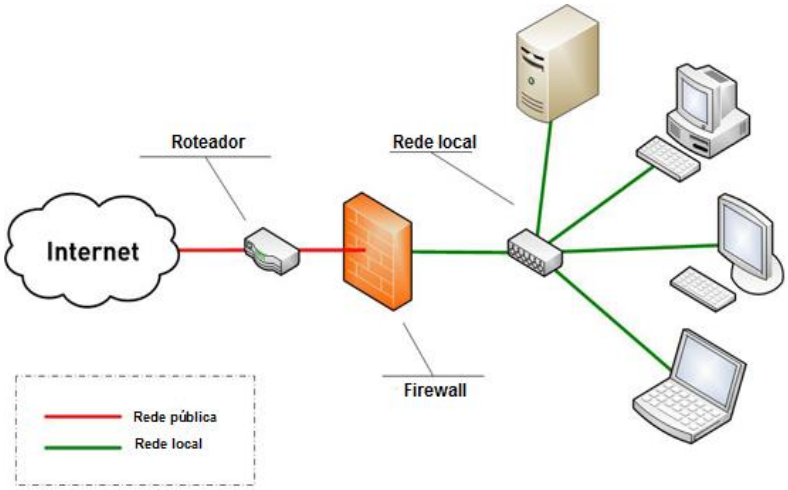
Nakamura e Lício (2007) afirmam que o processo de proteção de rede tem como ferramentas de auxílio o firewall, regras de filtragem o modelo hierárquico, que apresentam técnicas, tecnologias e arquiteturas que se enquadram melhor em cada situação.

3. FIREWALLS

Visto que a Internet não é uma rede confiável e carrega conteúdos mal-intencionados, Goodrich e Tamassia (2013) afirmam que Firewalls podem ser usados como um filtro da entrada e saída de conteúdo da Internet, através de diversas regras conhecidas como Política de Firewall, que ajudam a proteger os computadores das Redes.

Firewalls tem a função de proteger as redes internas de ataques que elas possam sofrer, e também de atuar como um modo de censura. Ou seja, o administrador da rede, tem o poder de bloquear o acesso de usuários da rede interna a certos sites, que podem conter conteúdos indevidos por meio da tecnologia de Firewall. Segue a **Figura 3.1** que mostrar como funciona essa aplicação:

Figura 3.1 Funcionamento do Firewall



NESETEC. **Tipo de Firewall**. Disponível em: <ttps://www.nesetec.com/index.php/2013/02/13/ventajas-al-usar-un-dispositivo-de-proteccion-firewall-en-la-red-de-la-empresa/>. Acesso em: 10 set.2017.

No caso da **Figura 3.1** acima há um exemplo de uma aplicação Firewall, a Internet vem através de uma rede Pública sendo roteada por ADLS e entra em contado com a Política de Firewall que trafega para outro roteador de rede local sendo distribuída para as demais máquinas com mais segurança.

3.1. CARACTERÍSTICAS DO FIREWALL

Stallings W. No livro Criptografia e segurança de Redes (2008), lista de alguns objetivos para o Firewall:

- Toda a informação necessariamente precisa passa pelo Firewall, de modo que todo o acesso à rede é bloqueado, menos através do Firewall.
- As políticas de Segurança controlam o que poderá ou não passar pelo Firewall
- O Firewall é impenetrável, portanto necessita de um sistema operacional seguro.

Lista também as técnicas utilizadas para controle de acesso através do Firewall:

- Controle de serviço determina o que pode ou não ser acessado na internet, filtrando a navegação através do endereço IP e a porta TCP.
- Controle de Direção, que delimita o caminha que o serviço tem que ser iniciado para que sua passagem pelo Firewall seja liberada.
- Controle de usuário controla o acesso a determinados serviços conforme o usuário que está utilizando a máquina.
- Controle de comportamento controla a maneira que os serviços são executados.

3.2. FUNCIONALIDADES

O Firewall possui diversas especificidades e cada uma delas com sua função, que interferem no nível de segurança do sistema. Nakamura e Lício (2007) definem algumas dessas especificidades como essenciais para um Firewall. Sendo elas, filtro, proxies, *bastion host*, zonas desmilitarizadas.

3.2.1. Filtros

Segundo Nakamura e Lício (2007), os filtros analisam os cabeçalhos e permitem ou bloqueiam o roteamento de pacotes, de acordo com regras definidas pela política de segurança estabelecida pelo administrador da rede. Nakamura e Lício (2007) afirmam também que os filtros comparam o conjunto de regras de segurança com as informações presentes no cabeçalho dos pacotes.

3.2.2. Proxies

Nakamura e Lício (2007) afirmam que Proxies são Gateways que tem a funcionalidade de trabalhar em duas redes, autorizando os pedidos e respostas dos usuários internos de acordo com a política de segurança previamente definida. Além disso, afirmam que os proxies podem ser como um *relay*, podendo agir como um filtro mais apurado dos pacotes por atuar na aplicação do modelo ISO/OSI (*International Orgaization* for *Standadization*/ *Open Systems Interconnection*).

3.2.3. Bastion hosts

Os serviços que são aplicados na internet são instalados e armazenados em objetos que são conhecidos como bastion hosts. Estes estão em contato direto com conexões externas, por isso precisam de proteção. De modo que o mesmo deve executar apenas aplicações realmente necessárias e sempre com correções de segurança prontas para serem aplicadas.

Nakamura e Lício, (2007) apontam os Bastion hosts também podem ser conhecidos como servidores fortificados, pois diminuem a vulnerabilidade dos pontos de ataque. Afirmam também que os bastion hosts estão em direto contato com a zona desmilitarizada (DMZ), já que os serviços oferecidos por esta, são instalados imediatamente nos bastion hosts.

3.2.4. Zona desmilitarizada

Segundo Nakamura e Lício, (2007) zona desmilitarizada é uma rede intermediaria entre a rede interna e externa. E tem a função de proteger a rede interna, sendo assim, se algum equipamento for corrompido na rede externa ou na rede desmilitarizada, a rede interna continua segura.

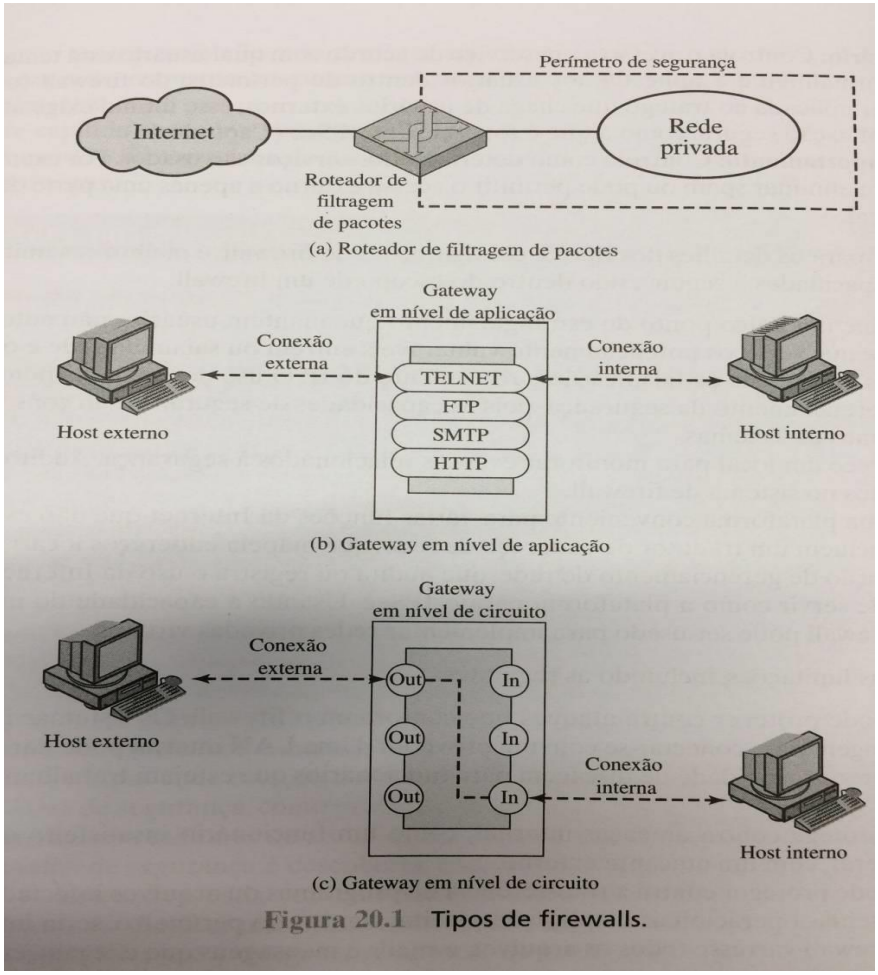
3.3. TIPOS DE FIREWALL

Segundo Stallings W, (2008), existem três tipos de Firewall:

- Filtro de pacotes, que é o roteador que aplicam diversas regra a cada pacote IP encaminhando ou bloqueando o pacote.

- Gateways em nível de aplicação, que é um servidor de transmissão de pacote dados também chamado de Proxy que dá autonomia ao administrador da rede em controlar os acessos dos usuários bloqueando determinados sites que podem trazer riscos.
    - Gateways com nível de circuito, que não permitem a conexão totalmente, ele cria duas conexões, uma interna e outra externa, e quando as duas conexões são estabelecidas, o conteúdo é transmitido sem análise. O Gateway em nível de circuito determina quais as conexões são permitidas ou bloqueadas.

Figura 3.2. Tipos de Firewall e como se aplicam.



Stallings, William – Livro. **Criptografia e segurança de Redes** 4ª Edição; Ano (2008). Pag. 446.

A Figura 3.2 - Acima ilustra as conexões da dos tipos de Firewall nos Hots internos e externos.

3.4. SISTEMAS CONFIÁVEIS DE FIREWALL

Stallings W, (2008), afirma que para proteger os computadores e os sistemas de ataques ou vírus que possam atingi-los, uma maneira eficaz é a implementação de uma tecnologia de sistemas confiáveis. E um método geralmente utilizado em organizações para proteção de seus dados é a Segurança multinível, onde camadas mais altas da organização tem acesso a informações que camadas mais baixas não têm.

Stallings W, (2008) diz também que para se obter a segurança multinível, é necessário seguir a duas regras, sendo elas: No *read up*, que significa nenhuma leitura acima, onde o indivíduo só tem acesso a informações de cargos abaixo ou iguais ao seu. E no *write down*, no português, nenhuma escrita abaixo, em que o indivíduo só pode escrever em um nível de segurança maior ou igual ao seu.

Além dessas duas regras, existe o monitor de referência que funciona controlando o acesso dos indivíduos a determinados objetos, baseando-se em um sistema de segurança do indivíduo e das informações. Stallings W, (2008) diz que o monitor de referência através do arquivo banco de dados *kernel* de segurança, tem o objetivo de controlar a segurança e proteção do objeto.

Segundo Stallings W, (2008), o monitor de segurança tem três propriedades, mediação completa onde as regras são aplicadas em cada acesso. Isolamento, onde é assegurado que não ocorrerá modificação inesperada. E Verificabilidade na qual poderá ser expressa matematicamente a imposição das regras de segurança.

4. CRIPTOGRAFIA

Se não realizadas corretamente, as políticas de segurança são ineficazes, e acabam deixando os computadores vulneráveis. Quando se diz respeito a ataques, as leis têm papel fundamental, porém, para atingir as metas de segurança e prevenir os riscos que podem afetar a empresa, é necessário contar com a eficácia de algumas soluções tecnológicas.

Segundo Goodrich e Tamassia, (2013), devem-se utilizar técnicas criptográficas para obter uma maior extensão de metas de segurança, acrescentando algumas extensões que inicialmente podem ser importantes.

A criptografia trabalha através de diversos meios de comunicação e segurança, visando tornar cada uma delas mais segura possível. A criptografia está presente nas organizações em várias ferramentas que são utilizadas para manter a segurança de informações como: assinatura de arquivos eletrônicos, transações bancarias, testes de identidade através de um servidor Web, segurança da movimentação de documentos, compras virtuais e segurança a de dados enviados por meio de Wi-fi. (Rede sem Fio).

4.1.1. Encriptação

Para se obter uma comunicação confidencial, Goodrich e Tamassia (2013) explicam sobre a encriptação, que seria uma maneira de duas ou mais pessoas terem acesso a uma informação privada em uma rede que não é segura.

Para enviar a mensagem com as informações confidenciais o sujeito que está enviando deve converter o arquivo utilizando um algoritmo de encriptação, escolhido de modo que só quem é autorizado tenha acesso, que fornecerá um texto cifrado, e este será transmitido. Assim, quando as pessoas autorizadas receberem a mensagem, aplicarão em tal mensagem algoritmo de decriptação que recuperará o texto original.

4.1.2. Criptossistemas

Na decriptação, deve ser utilizada alguma informação conhecida apenas por quem terá acesso a tal mensagem, a chamada chave de decriptação. Porem, Goodrich e Tamassia (2013) afirmam que para que funcione, é necessário que as pessoas envolvidas estejam de acordo com os textos, chaves de encriptação de

decriptação e algoritmos de encriptação e decriptação. Que formam um criptossistema.

4.1.3. Encriptação simétrica

Em uma criptografia simétrica, a mesma chave é utilizada para a encriptação quanto para a decriptação, Segundo Goodrich e Tamassia (2013), o *U.S.National Intitute* os *Standards* e *Technology* (NIST), recomendam a utilização do algoritmo Padrão de encriptação avançada. A característica de tal algoritmo é a velocidade com que é executado, entretanto não se associa com a assinatura e a certificação digital. Além disso, Nakamura e Lício (2011) falam que existe um problema na distribuição das chaves secretas a serem utilizadas pelos usuários, pois o meio de comunicação é inseguro. Existe também uma complexidade no controle das chaves secretas, pois cada mensagem e um dos meios de comunicação necessitam de sua chave secreta, sendo assim cada usuário pode ter diversas chaves secretas para gerir.

4.2. CIFRAS TRADICIONAIS

São alterados e os caracteres e os bit’s da mensagem um de cada vez, desconsiderando sua estrutura linguística, formando assim as cifras. Segundo Forouzan (2010), as cifras de chave simétrica tradicional podem ser separadas em: cifras de substituição e cifras de transposição.

4.2.1. Cifra de Substituição

Segundo Forouzan (2010) a Cifra de substituição se dá pela troca de símbolo por outro. Quando o símbolo utilizado for uma letra, ele é substituído por outra letra, quando é um número, é substituído por outro número distinto, e assim sucessivamente. Forouzan (2010) afirma que as cifras de substituição podem ser monoalfabéticas ou polialfabéticas.

- **Cifra monoalfabética:** Na cifra monoalfabética, em qualquer lugar do texto claro e do texto cifrado, os caracteres sempre são modificados para um mesmo caractere. Ou seja, se a letra A será trocada pela letra B, todas as letras A do texto serão modificadas para B.

- **Cifras polialfabéticas:** Nas cifras polialfabetica, os caracteres recebem substitutos distintos. Sendo assim, cada caractere no texto claro pode receber diversos substitutos no texto cifrado.
- **Cifra com Deslocamento:** também conhecida como cifra de César, é uma cifra monoalfabética simples, onde são usados apenas às letras do alfabeto e para criptografia e decriptografia são deslocados os caracteres de acordo com a chave. Se a chave for igual a três o algoritmo é deslocado três vezes para baixo ou para cima, para criptografia e decriptografia respectivamente.

4.2.2. Cifras de Transposição

Na cifra de transposição diferente da cifra de substituição, Forouzan (2010) diz que ocorre a mudança de posição dos caracteres. Os símbolos são reordenados e agrupados em blocos. A chave para as cifras de transposição é uma verificação das posições dos caracteres no texto claro e no texto cifrado.

4.3. ATAQUES.

Criptoanálise segundo Goodrich e Tamassia (2013), é o nome dado à ciência de ataques aos criptossistemas e as pessoas que atacam são os criptoanalistas. Na criptoanálise, o criptoanalista conhece os algoritmos de encriptação e decriptação, porém, as palavras chaves utilizadas lhe são uma incógnita. Porém, não é seguro confiar que as informações estão seguras considerando a confidencialidade dos algoritmos utilizados, pois não é difícil que essas informações vazem, dando assim, acesso ao criptossistema por parte do criptoanalista.

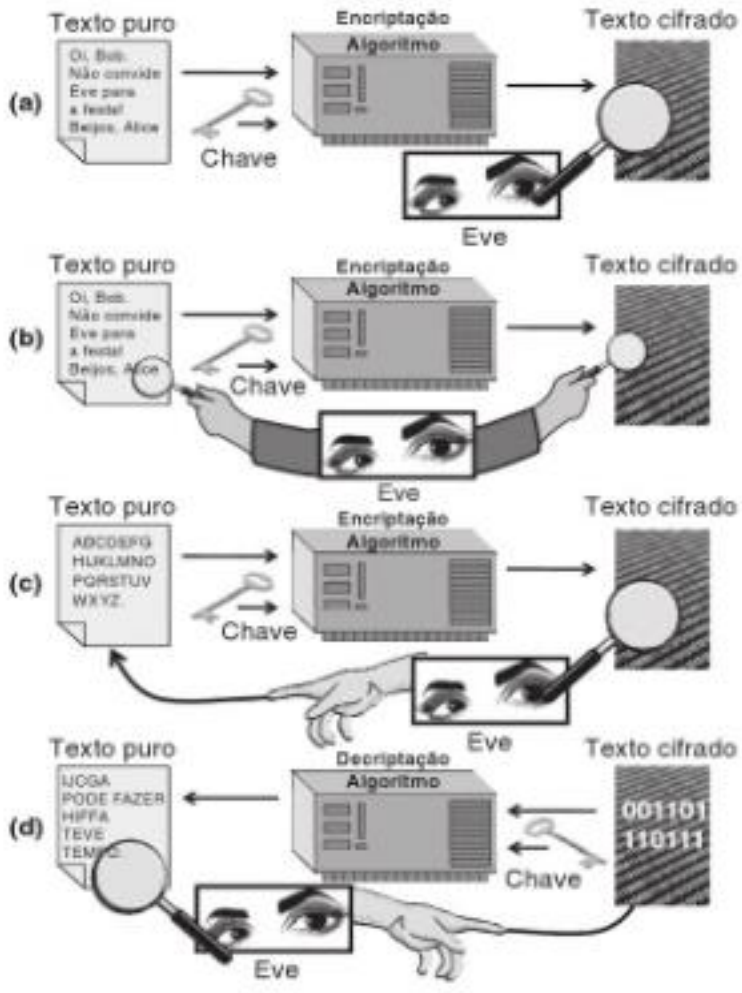
Goodrich e Tamassia (2013) explicam que documentos internos de uma organização podem ser publicados ou furtados, e o desenvolvedor que codificou um algoritmo pode passar alguma informação, ou até um sistema de software ou hardware que executa um algoritmo de encriptação pode sofrer engenharia reversa.

O criptossistema pode sofrer com quatro tipos de ataques por parte do criptonalista. São eles:

- **Ataque ao texto cifrado** – onde o criptoanalista tem acesso ao texto cifrado de uma mensagem que foi encriptado por uma chave, e seu objetivo é descobrir o texto puro ou a chave que foi utilizada.

- **Ataque ao texto puro conhecido** – em que o criptoanalista consegue acesso a um par que contém o texto puro e o texto cifrado, e seu objetivo é descobrir a chave usada.
- **Ataque ao texto puro escolhido** – o criptoanalista escolhe uma mensagem em texto puro e obterá o texto cifrado através da chave utilizada.
- **Ataque ao texto cifrado escolhido** – o criptoanalista escolhe a mensagem em texto cifrado e através da chave que está associada ao mesmo descobre texto puro.

Figura 4.1 – Tipos de Ataques



GOODRICH, Michael T, TAMASSA, Roberto. Livro. **Introdução à Segurança de Computadores**. Bookman; Ano (2013). Pag. 384.

Figura 4.1 Acima mostra os tipos de ataques: a) ataque ao texto cifrado; b) ataque ou texto puro conhecido; c) ataque ao texto puro escolhido; d) ataque ou texto cifrado escolhido. Programas maliciosos (malware).

5. PROGRAMAS MALICIOSOS (MALWARE)

Existem aparelhos que fazem conexão a internet para envios de dados, e isso fornece vantagens como, conectar a um site, enviar e-mail, recursos de músicas online, ligações e vídeos em tempo real. Mas toda essa tecnologia também contém programas maliciosos.

Softwares maliciosos são programas que em sua execução trazem consequências prejudiciais e involuntárias para o computador. Malware é o nome dado a softwares maliciosos que podem atingir os sistemas.

De acordo com Goodrich e Tamassia (2013), o ataque interno pode ocorrer quando o código do ataque vem em um programa que é parte do sistema operacional ou um programa que é instalado por um usuário ou administrador do sistema.

Um ataque interno se dá devido a uma falha de segurança que ocorre quando um programador ou um funcionário da organização facilita o ataque, deixando a rede vulnerável. Um ataque interno é extremamente perigoso por ser desencadeado por um funcionário da empresa, que é alguém que conhece os dados que devem ser protegidos e ainda assim facilita o ataque.

Goodrich e Tamassia (2013) dizem que quando o Malware afeta um aparelho ele pode causar danos como, instalar *spyware*, que captam as informações sigilosas e também deixa o sistema exposto a um sistema chamado *botnet*, que se trata de uma rede se máquinas comprometidas controladas por um vilão que espalha spam ou ataques nos aparelhos da rede.

Ross. K (2010) no livro, Redes de Computadores e a Internet, fala que muitos malwares presentes são multiplicados constantemente, utilizando-se de hospedeira já infectada para transmitir para outro hospedeiro, sendo assim o malware pode alastrar rapidamente.

5.1. DEFESAS CONTRA ATAQUES INTERNOS.

As defesas do sistema contra os ataques internos são difíceis, já que o malware é instalado por uma pessoa na qual a empresa deposita sua confiança. Porém, segundo Goodrich e Tamassia (2013), existem algumas formas das organizações tentarem proteger os sistemas. São elas:

- Não permitir que um único funcionário seja responsável pela criação de backups e gerenciamento de recursos.
- Orientar que os programadores se comuniquem de modo que trabalhem juntos e conheçam os códigos uns dos outros, para que se ajudem e encontrem erros ou omissões antes não vistos, sendo assim um programador não será capaz de fazer nenhuma alteração sem que seja descoberto por outro programador.
- O uso de ferramentas de arquivamento e documentação. São ferramentas que criam ícones visuais ou condensa arquivos tornando mais fácil para ser revisados fazendo que o malware seja percebido com maior facilidade.
- Estabelecer o limite de autoridade e permissão, de modo que o funcionário só tenha acesso ao que é necessário para realizar suas tarefas com eficiência.
- Monitoramento do comportamento de funcionários, especialmente programadores.
- Controle de instalação de softwares, certificando-se que softwares e programas instalados sejam de fontes confiáveis.

Seguindo as orientações propostas por Goodrich e Tamassia (2013), as organizações ficam mais seguras e correm menos riscos de sofrer com ataques internos.

5.2. VÍRUS DE COMPUTADOR

Vírus é o nome dado a um código de computador que se multiplica através da modificação de diversos arquivos e programas onde insere o código que se replica posteriormente. Um vírus necessita de uma ajuda do usuário para conseguir entrar no computador, como clicar em um link, e-mail infectado ou até mesmo uma unidade USB que esteja infectada. E causa danos como perda de arquivos e até mesmo acesso e roubo de senhas.

Goodrich e Tamassia (2013) afirmam que os vírus de computador são como os vírus biológicos, e é usado o mesmo o termo “Vetores biológicos” para se referir as vulnerabilidades que um Malware com vírus de computados, utiliza para realizar os ataques.

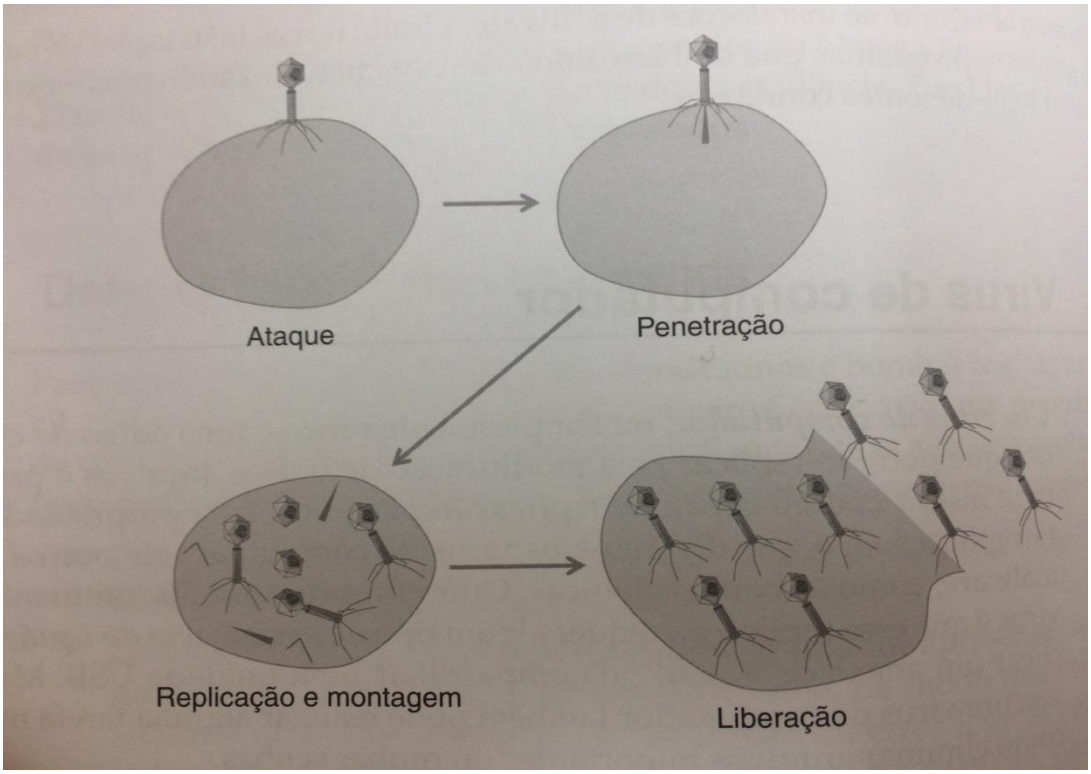
Quando liberados, os vírus se alastram para programas do computador que não estão infectadas pelo vírus. Em alguns casos o vírus entra em *stand-by*, esperando por um tipo específico de programa que não esteja infectada. Quando o encontra, é executado e se multiplica junto com ele, sendo produzido em grande quantidade.

5.2.1. Classificação de vírus.

Segundo Goodrich e Tamassia (2013) existem quatro fases de execução dos vírus de computador, são elas:

- **Fase dormente**. É quando o vírus fica em *stand-by*, sem fazer nenhuma infecção.
- **Fase de propagação**. Nessa fase o vírus está se alastrando, infectando dados e softwares.
- **Fase de ativação**. Trata-se de quando vírus se utiliza da fase dormente ou da fase de propagação para fins de ação pretendida.

Figura 5.1 - Fases do vírus biológicos



GOODRICH, Michael T, TAMASSA, Roberto. Livro. **Introdução à Segurança de Computadores**. Bookman; Ano (2013). Pag. 178.

Figura 5.1 – Mostra o funcionamento de cada fase do vírus biológicos.

- **Fase de ação**. Nesta fase é quando o vírus executa o procedimento malicioso para que fosse criado

Goodrich e Tamassia (2013), falam que “os vírus de computadores se caracterizam de várias formas. Uma forma de classificar variedades de vírus é pelo tipo de dados que ele infecta”.

5.2.2. Tipos de Vírus.

Goodrich e Tamassia (2013) explicam um pouco sobre os tipos de vírus que podem atingir os computadores. Falam que o vírus que atinge um programa modificando o arquivo que contém seu código objeto é conhecido como vírus de programa ou vírus de arquivo. Onde, após um programa ser infectado, o vírus é executado junto com o programa, sendo assim, se o programa for executado constantemente, o vírus tem maior probabilidade de se manter e de se replicar. Portanto, os programas mais utilizados são os alvos naturais dos ataques por tal tipo de vírus.

Goodrich e Tamassia (2013) explicam também que os programas que trabalham com documentos como o Word, utilizam sistema que automatizam as sequências de comandos, que facilitam na atualização automática de fatos, fotos, nomes e datas, à medida que tal informação seja alterada. Tais sistemas atuam de maneira parecida a um programa executável, portanto acaba por se tornar alvo de vírus.

Outro tipo de vírus citado por Goodrich e Tamassia (2013) é o Vírus de Macro ou Vírus de documento, que aparece no momento em que um documento é aberto e então procura outros documentos vulneráveis para infectar. Tais documentos podem ser enviados e infectar outros usuários.

Por último afirmam também sobre o Vírus de setor de carga (boot sector), que infecta o código no setor de carga de uma unidade, e sempre que o computador é ligado, o vírus é executado.

5.3. DEFESAS CONTRA VÍRUS.

Goodrich e Tamassia (2013) afirmam que os vírus de computador se apresentam da mesma forma que o vírus biológico, em que os nossos corpos reagem a estranhos nefastos. No momento que o vírus infecta o corpo do indivíduo

e obtém a passagem pelas suas defesas, ele consegue infectar rapidamente muitas das suas células. Porém, à medida que o vírus se propaga, o sistema imunológico age no corpo e monta sua própria defesa conforme as características do vírus e trabalha para restaurar as células infectadas.

Segundo Goodrich e Tamassia (2013) “A forma que um vírus se espalha e infectam rapidamente são quando ficam livremente se movimentando pelas defesas de cada sistema sem que eles percebam“. Essa infecção irremediavelmente é percebida pelo analista de segurança de sistema, que por sua vez envia esses vírus localizados para o setor de antivírus. Os especialistas analisam os dados danificados, e procura por códigos peculiar sendo um vírus de computador. Se confirmado qual fragmento de código atacou os arquivos os analistas constroem um *string* de caracteres que localizam o vírus.

5.3.1. Vírus encriptados.

Os programas de Antivírus têm como principal objetivo as assinaturas de vírus. Sendo assim, os códigos dos vírus são camuflados, na tentativa de não serem descobertos. Como dito por Goodrich e Tamassia (2013), os vírus podem ser divididos, colocados em diferentes posições, na tentativa de camuflar o código do vírus que se espalha pelo arquivo inteiro. Porém, basta juntar as peças do vírus para descobrir o seu código.

O código de um vírus carrega consigo muitas informações como o código de replicação e à sua carga, e tais informações acabam escondidas através da encriptação. Que segundo Goodrich e Tamassia (2013), “tem como objetivo dificultar que os programas de antivírus encontrem e eliminem o vírus”.

5.4. BOAS PRÁTICAS.

Existem vários tipos de cuidados que podem ser utilizados para proteger programas contra malwares. Goodrich e Tamassia (2013) informam que “as melhores formas de práticas inferidas são”:

- Obter, diversos sistemas como operacional, sistema que elabora documentos, sites Web, sistema de execução de imagem ou vídeo. Sendo utilizadas essas variedades de sistemas a vulnerabilidades de características de softwares podem ter uma diminuição de danos.

- Estabelecer instalações de softwares de fontes confiáveis, para não causar preocupações e dor de cabeça para as organizações, empresas que podem ter sua vulnerabilidade exposta para o malware.
- Desligar a autoexecução. Deixar a autoexecução é um risco desnecessário para a empresa. Sendo que podem ser executados manualmente.
- Adotar o princípio do menor privilégio, onde os funcionários tenham acesso somente aos privilégios necessários para realização de seu trabalho, ajudando a evitar ataques de escalação de privilégios.

Essas são boas práticas que Segundo Goodrich e Tamassia (2013) ajudam as organizações a se protegerem contra os Malware.

5.4.1. Boas praticas adicionais.

Para proteger os computadores e sistemas contra a invasão de vírus e diminuir os danos provocados por eles, Goodrich e Tamassia (2013), no livro Segurança de Redes do Ambiente corporativo, falam sobre boas práticas, que são:

- Evitar *freware* e *shareware* que não tenham garantias e boa reputação. Indicam que é importante que o software seja assinado digitalmente, de modo que a integridade possa ser verificada utilizando funções criptográficas.
- Evitar sistemas de compartilhamento de música e vídeos, que muitas vezes contém vírus.
- Adquirir um monitor que impeça a instalação de softwares maliciosos e download de páginas web com Malwares.
- Instalar um Firewall que bloqueie a transmissão de dados não permitidos.
- Utilizar outros métodos além da senha para proteger uma conta de usuário, como biometria, cartões inteligentes, entre outros.
- Manter todos os programas atualizados com as últimas correções de segurança, para dificultar que sejam encontradas vulnerabilidades.
- Evitar que sejam utilizadas senhas fracas.
- Utilizar programas de detecção de erros e Malwares.

Se todas essas boas práticas forem seguidas com êxito, a chance de danos provocados por vírus atingirem os computadores diminuirá significativamente.

6. POLÍTICA DE SEGURANÇA

As Políticas de segurança são fundamentais para as organizações quando se diz respeito à proteção da informação. É necessária muita atenção no planejamento e elaboração das políticas de segurança, já que é através delas que são definidos todos os programas responsáveis pela segurança dos recursos.

Segundo Nakamura e Lício (2007), as Políticas de segurança trabalham com a legislação local, com os negócios e também com os processos. De modo que abrange diversos aspectos da organização como aspectos humanos, culturais e tecnológicos. Sendo assim, as normas e procedimentos da organização devem ser baseados na política de segurança.

Uma vez que uma organização implanta a política de segurança, esta tem o objetivo de facilitar e simplificar o gerenciamento dos recursos da organização. E Nakamura e Lício (2007) afirmam também que o gerenciamento de segurança é a arte da criação e administração de políticas de segurança, pois não dá para gerenciar aquilo que não pode ser definido.

6.1. O PLANEJAMENTO.

As Políticas de segurança precisam de um planejamento prévio para que os riscos sejam compreendidos e evitados. Quando pensado em segurança deve-se pensar na reação pode trazer riscos para a organização. Nakamura e Lício (2007) falam que uma política de segurança tem que ser pró-ativa e necessita que a política de segurança seja bem definida. As responsabilidades de cada membro da organização devem ser bem esclarecidas, para que o gerenciamento de segurança seja mais simples para as organizações.

As organizações precisam do apoio de executivos para que as tenham recursos financeiros para realizar as soluções necessárias. Os executivos se mostram comprometidos quando existe uma política de segurança defina e bem planejada, Nakamura e Lício (2007) dizem que é importante à aprovação dos executivos à política de segurança na organização, e também é importante que ela seja publicada e comunicada a todos os membros da organização.

A política de segurança deve ser planejada de modo que inclua todos os setores da organização inclusive as regras a serem seguidas. Nakamura e Lício (2007)

Tais regras devem falar quais funcionários tem acesso a determinadas informações e os procedimentos que auxiliam a proteção das informações.

De acordo com Nakamura e Lício (2007), as políticas de segurança podem ser divididas em alguns níveis, o mais básico para que os executivos entendam o nível dos usuários para, que os mesmos conheçam as contribuições que podem dar para segurança da organização e o nível técnico que diz respeito a conhecimentos específicos e implementação de regras de filtragem.

6.2. OS ELEMENTOS.

Uma política de Segurança deve ter como elementos tudo o que é necessário para combater os problemas. Não se diz respeito apenas a vírus e hackers, a infraestrutura da organização.

Nakamura e Lício (2007) citam elementos essenciais da política de segurança e de sua implementação. Alguns desses elementos são:

- Vigilância: que diz que todos os funcionários devem zelar pela segurança da organização, atuando como guardiões da rede, ajudando a monitorar os sistemas e as redes.
- Atitude: que é a postura e conduta quanto à segurança. A atitude é inspirada pelo treinamento, sendo assim, é essencial que a política de segurança definida seja de fácil acesso a todos e que todos os funcionários compreendam e se tornem cúmplices da organização.
- Estratégia: que diz respeito à definição da política e do plano de defesa da organização, e à habilidade de se adaptar as mudanças. A estratégia deve analisar a produtividade dos funcionários, para que as medidas de segurança não prejudiquem os negócios da organização.
- Tecnologia: as tecnologias precisam ser flexíveis, para acompanhar as estratégias da organização. A organização deve adquirir uma política de segurança dinâmica, em que várias tecnologias e práticas são adotadas.

Para Nakamura e Lício (2007), a vigilância, atitude, estratégia e tecnologia são os fatores essenciais da política de segurança.

A ISO/IEC 17799 estabelece normas de segurança que necessitam ser seguidas nas políticas de segurança. Algumas delas são:

Nakamura e Lício (2007) afirmam que a política de Segurança é definida, com metas, escopo e a importância da segurança, salientando o papel de mecanismo que possibilita a divulgação da informação e o sucesso da organização. Outra orientação a ser seguida é a declaração de apoio dos executivos, e um esclarecimento das políticas e princípios de segurança da organização. Devem se definir também as responsabilidades no controle da segurança, regras para usuários e procedimentos de segurança devem ter como base políticas e normas mais detalhados sistemas específicos.

A política de segurança não deve possuir técnicas específicas utilizadas cada indivíduo, e sim regras utilizadas pelas organizações de maneira geral. Nakamura e Lício (2010) dizem que para evitar que alterações frequentes ocorram na política de segurança, é necessário que a política seja flexível para compreender possíveis exceções.

Todos os funcionários de uma organização devem ter acesso e ler toda a política de segurança, portanto, é necessário que ela seja breve e o mais direto possível. É importante também que a política apresente normas e procedimentos direcionados para cada setor da empresa.

6.3. A IMPLEMENTAÇÃO.

A implementação é a parte mais complexa da política de segurança, sua origem envolve conhecimento, ambiente de rede, cultura, tecnologia, pessoas e organizações, sendo assim é um processo trabalhoso e difícil. Mas a maior complexidade é que os indivíduos que trabalham na organização têm que conhecer a política e as mudanças e aceitá-las, de modo que a implementação ocorra com êxito. Nakamura e Lício (2010) dizem que então, um ponto importante para que ocorra a implementação é a educação, pois a falta de conscientização dos funcionários acaba por tornar a política inoperante ou ineficaz.

É importante que a política de segurança se torne parte da cultura da organização. Para que todos tenham consciência das regas e os controles básicos de segurança. Nakamura e Lício (2010) falam que a divulgação pode ser feita através de e-mails, painéis treinamentos, peças teatrais, entre outras.

A implementação de uma segurança demora anos para ter os resultados esperados. E são necessários muitos esforços para que o planejamento seja

aprovado em longo prazo. Nakamura e Lício (2010) falam que a organização deve reservar um valor no orçamento voltado para a segurança. Contando com o planejamento, equipes e dependências. E a segurança deve ser considerada essencial, como qualquer outro setor, pois é uma ferramenta estratégica para a organização.

Vale salientar que ao contrário do que as pessoas pensam, a implementação da segurança diminui os custos das operacionais da empresa, já que ajuda a evitar problemas e controlar os recursos da organização.

Nakamura e Lício (2010) afirmam que a partir do momento em que todos os funcionários tenham conhecimento da política de segurança e a coloquem em prática, é necessário que todos sejam observados e verificados de acordo com a política. Tal verificação pode ocorrer na forma de auditorias. O descumprimento das normas impostas na política de segurança deve ser punido.

Além da auditoria, Nakamura e Lício (2007) falam que é necessário fazer o monitoramento e a revisão da política, para a melhoria da segurança da organização. E são necessários também em qualquer mudança como incidentes na segurança, aparecimento de vulnerabilidades ou mudanças na infraestrutura da organização. A partir daí a manutenção da política de segurança podem ser realizados, novos métodos de segurança podem ser adicionados ou retirados da política.

6.4. POLITICA DE SEGURANÇA NO AMBIENTE CORPORATIVO.

Com o desenvolvimento da organização surge uma necessidade de uma de política de segurança que acompanhe seu conhecimento. A política de segurança de uma organização deve corresponder como a sua cultura, sendo assim, é importante que cada empresa tenha uma política própria. Nakamura e Lício (2007) afirmam que a fusão de várias políticas diferentes pode ser fatal para a segurança da empresa.

Nakamura e Lício (2007) citam como exemplo três empresas diferentes sendo as empresas 1,2 e 3. Cada uma delas possui uma política de segurança especifica. Na empresa 1 a política permite que os membros da empresa 3 acessem o seu sistema, entre tanto a empresa 2 está proibida de acessar o sistema. Na política da empresa 3 ela permite que membros da empresa 2 utilizem sua rede. Sendo que dessa forma membros da empresa 3 tem acesso ao sistema da 1 e através da

empresa 3, os membros da 2 conseguem acessar a rede da empresa 1. Sendo assim burlado a política de segurança na empresa 1.

Nakamura e Lício (2007) falam que no ambiente corporativo esse tipo de transtorno passa ser um fator comum, entretanto isso pode mudar se houver uma concordância mútua, sendo pré-definida, através das políticas do ambiente corporativo. A forma que isso ocorre é que quando a organização 3 através de uma ponte fornece acesso aos membros da organização 2 por um protocolo conhecido como Telnet. Portando os membros da 2 podem acessar a organização 1, sendo que não é permitido. Somente se a organização 1 for convencida a bloquear a utilização do Telnet, o que dificilmente pode ocorrer.

Esses problemas podem ser minimizados com a adoção de uma política de segurança em comum. Essa adoção, porém, enfrentará grande dificuldade no desenvolvimento e implementação. Pois é complicado assegurar que os membros da organização cumpram tudo o que diz a política de segurança. O que torna esse pensamento ineficaz, voltando à ideia de que cada organização tenha sua política própria.

7. CONSIDERAÇÕES FINAIS

O Estudo abordado no trabalho mostra como as organizações, empresas e o ambiente corporativo estão vulneráveis em relação à segurança das informações. Quando o assunto é segurança de redes devem ser pensado na internet e outros meios de comunicação. Porém, é através da rede que vem as maiores preocupações para organização, expondo assim a confidencialidade, integridade e disponibilidade da mesma.

Dessa forma, foram apresentadas algumas maneiras de proteger as redes contra quaisquer perigos que podem tentar atingi-las. Uma dessas maneiras Firewall que pode ser considerado um filtro na entrada e saída de conteúdos através da internet, e também permite que o administrador da rede controle quais conteúdos podem ou não ser acessados pelos usuários. Outro método que pode ser utilizado na proteção das informações é a Criptografia, que é uma forma de usuários trocarem informações em uma rede de comunicação que não é segura codificando os dados de forma que somente eles tenham acesso.

Foram estudados alguns programas maliciosos conhecidos como Malware. Indivíduos fazem o uso de sites, e-mail, downloads de músicas, filmes e dessa forma ficam expostos a programas maliciosos, porem existem maneiras de se proteger do Malware, como programas de antivírus e algumas medidas propostas aos funcionários da organização.

Para construir uma organização, e um ambiente corporativo seguro, é importante que cada organização construa uma política de segurança, que abrange todos os recursos da organização, como normas, leis, cultura, e aspectos humanos. A política de segurança tem o objetivo de ajudar no gerenciamento da organização, e se política de segurança for comprida fielmente a organização se torna muito mais segura.

Portanto, é importante que as organizações invistam em segurança, criando uma boa política, que os usuários tenham conhecimento e a sigam com rigor. E, além disso, investir em programas que evitem ataques externos, como vírus, hackers e outros perigos que possam atingi-las através das redes. Tomando essas precauções, as corporações enfrentarão menos dificuldades para manter seguros os seus dados.

8. REFERÊNCIAS

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores 4ª Edição.** Brasil. AMGH Editora. 2010.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. Brasil. Bookman. 2013.

NAKAMURA, Emilio Tissato; LÍCIO, Paulo. **Segurança de Redes em Ambientes Cooperativos.** Brasil. Novatec, 2007.

NESETEC. **Tipo de Firewall**. Disponível em:<ttps://www.nesetec.com/index.php/2013/02/13/ventajas-al-usar-un-dispositivo-de-proteccion-firewall-en-la-red-de-la-empresa/>. Acesso em: 10 set.2017.

ROSS. Kurose. **Redes de Computadores e a Internet 5ª Edição**. Brasil. Pearson, 2010.

STALLINGS. William. **Criptografia e Segurança de Redes 4ª Edição.** Brasil. Pearson, 2008.

TANENBAUM, Andrew S. **Computer Networks**. 4ª. Ed. Estados Unidos da Amarica: Prentice Hall, 2002.