Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Paulo Affonso Gouveia Cabral Junior

UMA ANÁLISE COMPARATIVA DA SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE DE PEQUENA EMPRESA

Rio de Janeiro

2007

Paulo Affonso Gouveia Cabral Junior

UMA ANÁLISE COMPARATIVA DA SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE DE PEQUENA EMPRESA

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof. Carlos Eduardo Mendes de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

2007

Paulo Affonso Gouveia Cabral Junior

UMA ANÁLISE COMPARATIVA DA SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE DE PEQUENA EMPRESA

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em Dezembro de 2007.

Carlos Mendes

Prof. Prof. Carlos Eduardo Mendes de Azevedo, M.Sc., UFRJ, Brasil

Por ter sido uma tarefa muito árdua, dedico este trabalho aos meus pais, pelo incentivo, colaboração e carinho que recebi durante a realização de toda Monografia.

AGRADECIMENTOS

Gostaria de agradecer ao meu amigo Rafael Brandão pela sua contribuição na realização do curso.

Ao professor Carlos Eduardo Mendes de Azevedo, por toda orientação, apoio e atenção fornecidas durante o desenvolvimento deste trabalho.

Ao Coordenador do curso Moacyr, que sempre me incentivou a realizar esse trabalho.

RESUMO

CABRAL, Paulo Affonso Gouveia. **UMA ANÁLISE COMPARATIVA DA SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE DE PEQUENA EMPRESA**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

O objetivo da pesquisa foi realizar um estudo que teve como foco principal, explicar como pequenas empresas, com baixo orçamento, podem conseguir um bom nível de segurança.

Por esse motivo foi utilizado o método Survey, que utilizou como fonte primária a coleta de dados, com profissionais que trabalham com segurança da Informação em diferentes cidades Brasileiras.

As soluções pesquisadas foram divididas em categorias e para se conseguir um melhor aproveitamento das informações coletadas, foram criadas tabelas utilizando-se fórmulas matemáticas para relacionar essas informações, especificando as soluções que tiveram melhores pontuações.

Após análise das informações coletadas, as soluções que atingiram o objetivo principal da pesquisa, foram as soluções de baixo custo, com bom nível de segurança. Na categoria Firewall, a solução da Check Point se destacou, conseguindo altas pontuações em todos os itens analisados. Na categoria Scanner de Vulnerabilidade, o software Nessus foi o destaque e na categoria IDS, a dificuldade de configuração e o custo, praticamente inviabilizaram sua utilização.

ABSTRACT

CABRAL, Paulo Affonso Gouveia Cabral. **UMA ANÁLISE COMPARATIVA DA SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE DE PEQUENA EMPRESA**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

The objective of this research has been to perform a study, which is mainly focused in explaining how the small companies, with a low budget, are able to achieve a good security level.

For that purpose we adopted the Survey method, which used, as its primary source, the collection of data together with the professionals who work with the security of information in different Brazilian cities.

The researched solutions were divided in categories, and in order to obtain a better use of the collected data, tables were created based on mathematical formulas to relate those data specifying the solutions that achieved the best grades.

After analyzing the collected data, the solutions achieved the main objective of the research. They were low cost solutions, with a good security level. In the Firewall category the Check Point solution stood out, obtaining high grades in all the analyzed items. In the Scanner of Vulnerability category, the Nessus software was the highlight. In the IDS category, the configuration difficulty and its cost, made its use practically not viable.

LISTA DE FIGURAS

Página

Ilustração 1 – Gráfico com as idades dos entrevistados 40
Ilustração 2 - Gráfico com os resultados obtidos na categoria Firewall 45
Ilustração 3 - Gráfico com os resultados obtidos na categoria Scanner de Vulnerabilidade 45
Ilustração 4 - Gráfico com os resultados obtidos na categoria Scanner de Vulnerabilidade Web 46
Ilustração 5 – Gráfico com os resultados obtidos na categoria IDS 49
Ilustração 6 – Gráfico com o percentual de Ataques por categoria 51
Ilustração 7 – Gráfico com o grau de Risco por categoria 52

LISTA DE QUADROS

	Página
Quadro 1 – Total de indicações na categoria Firewall	42
Quadro 2 – Total de pontos com a classificação da categoria Firewall	44
Quadro 3 - Total de pontos com a classificação dos Scanners de Vulnerabilidades	46
Quadro 4 - Total de pontos com a classificação dos Scanners de Vulnerabilidades Web	47
Quadro 5 - Total de pontos com a classificação dos IDS	48
Quadro 6 – Percentual de Ataques por categoria	50
Quadro 7 – Grau de Risco dividido por categoria	52

LISTA DE ABREVIATURAS E SIGLAS

ACL	Access Control List
ARP	Address Resolution Protocol
ASA	Adaptive Security Appliances
CSS	Cross Site Scripiting
DDOS	Distribuied Denial of Service
DMZ	Desmilitarized Zone
DNS	Domain Name Server
FTP	File Transfer Protocol
HIDS	Host-Based intrusion detect system
HIPS	Intrusion Prevent System
HTML	Hyper Text Markup Language
HTTP	Hyper Text Markup Language
ICMP	Internet Control Message Protocol
IDS	Intrusion Detect System
IP	Internet Protocol
ISA	Internet Security and Aceleration Server
NIDS	Network Intrusion Detect System
OSI	Open Systems Interconnection
PF	Packet Filter
RPC	Remote Procedure Call
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTM	Unified Threat Management Perfomace
WWW	World Wide Web

SUMÁRIO

Página

1 **INTRODUÇÃO** 13
1.1 MOTIVAÇÃO 13
1.2 OBJETIVOS 14
1.3 RELEVÃNCIA 15
1.4 ORGANIZAÇÃO DO TRABALHO 15
2 **REFERENCIAL TEÓRICO** 17
2.1 CONSIDERAÇÕES INICIAIS 17
2.2 TIPOS DE ATAQUES 17
2.2.1 **Ataques de Negação de Serviço** 17
2.2.2 **Buffer Overflow Attack** 18
2.2.3 **SYN Attack** 19
2.2.4 **Teardrop Attack** 19
2.2.5 **Smurf** 19
2.2.6 **Corrida contra o tempo** 19
2.2.7 **SQL Injection** 20
2.2.8 **PHP Injection** 20
2.2.9 **Cross Site Scripting** 20
2.2.10 **Engenharia Social** 20
2.2.11 **Analisadores de Portas "PortScanners"** 21
2.2.12 **Ataques de Botnets** 21
2.2.13 **Spoofing de Arp** 22
2.2.14 **DNS Spoofing** 22
2.2.15 **Zero day Vulnerabilities** 22
2.3 DESCRIÇÃO DAS PRINCIPAIS TECNOLOGIAS DE FIREWALLS 23
2.3.1 **Filtro de Pacotes Estáticos** 23
2.3.2 **Nível de Aplicação** 24
2.3.3 **Estado de Conteúdo** 24
2.3.4 **Filtro de Pacotes Dinâmico** 25
2.3.5 **Kernel Proxy** 25
2.4 ARQUITETURAS DE FIREWALL 25
2.4.1 **Screening Router** 25
2.4.2 **Dual-hommed Host** 25
2.4.3 **Screened Host** 26
2.4.4 **Screened Subnet (DMZ)** 26
2.5 DESCRIÇÃO DOS TIPOS DE IDS 26
2.5.1 **Informações Importantes para Analisar um IDS** 28
2.6 SCANNERS 30
2.6.1 **Scanners de Vulnerabilidades** 30
2.6.2 **Scanner de Rede** 30
2.6.3 **Scanner de Host** 30
2.7 PRINCIPAIS AMEAÇAS DE REDE 31
2.7.1 **Ataques Internos** 31
2.7.2 **Ataques Externos** 31
3 **METODOLOGIAS DE PESQUISA** 33
3.1 INTRODUÇÃO 33
3.2 TIPO DE PESQUISA 33

3.3 MODELO DE REFERÊNCIA DA PESQUISA 35
3.4 HIPÓTESES 35
3.5 UNIVERSO E AMOSTRA 36
3.6 COLETA DE DADOS 37
3.7 ANÁLISE E INTERPRETAÇÃO DOS DADOS 37
3.8 LIMITAÇÕES DO MÉTODO 38
4 **RESULTADOS** 39
4.1 ANÁLISE DESCRITIVA DA AMOSTRA 39
4.2 ANÁLISE DOS ITENS DO QUESTIONÁRIO 40
5 **CONCLUSÃO** 54
5.1 CONTRIBUIÇÕES 54
5.2 LIMITAÇÕES DA PESQUISA 60
5.3 TRABALHOS FUTUROS 60
REFERÊNCIAS 61

1 **INTRODUÇÃO**

1.1 **MOTIVAÇÃO**

A principal motivação do trabalho foi a realização de uma pesquisa com objetivo de orientar como Pequenas Empresas, com baixo orçamento, podem garantir um bom nível de segurança.

Essas empresas utilizam Internet, redes sem fio, softwares de alta complexidade, o que aumentou muito as vulnerabilidades encontradas, percebe-se que é necessário, quando for realizado algum tipo de investimento com segurança da informação, uma orientação a fim de que os investimentos sejam destinados para as melhores tecnologias.

Atualmente existem servidores sendo implementados em ambientes de produção, sem ser realizado uma análise crítica da segurança desses servidores, uma análise crítica das infra-estruturas onde estão sendo instalados. Percebe-se que os cenários que se têm hoje, são de empresas, implementando redes inseguras, servidores com alto grau de vulnerabilidade, e softwares desenvolvidos e configurados de forma incorreta.

Como a informação, assim como qualquer outro bem, tem um relevante valor, podendo ser o principal ativo de uma Empresa, é necessário estruturar a segurança dessas informações. Conclui-se que, é necessário que as informações sejam preservadas com alto grau de segurança.

Logo é necessária à utilização de softwares de segurança de baixo custo, com facilidade de configuração, ampla eficácia e abrangência de defesa. Com este objetivo será realizada uma pesquisa, com profissionais da área de Segurança da

Informação, para coletar informações das soluções que esses profissionais indicam, e recomendações para melhorar a infra-estrutura dessas empresas.

1.2 **OBJETIVOS**

O objetivo da pesquisa foi realizar um estudo que teve como foco principal, explicar como pequenas empresas com baixo orçamento, podem conseguir um bom nível de segurança.

Essa pesquisa também tem como finalidade contribuir e ajudar essas empresas a definir soluções de segurança, que sejam compatíveis com o seu orçamento. O trabalho irá utilizar como fonte primária a coleta de dados junto a Empresas de Segurança de Informação e profissionais de segurança.

Além dessas informações será realizado um levantamento dos principais tipos de ataques, que essas empresas estão sujeitas a receber, explicando o motivo e as possíveis causas, visto que será realizada uma coleta de dados em diferentes Estados do País, centralizando a pesquisa nas seguintes cidades: Rio de Janeiro, São Paulo, Recife e Fortaleza.

Com os dados coletados, serão realizadas estatísticas de cada categoria, e nas soluções que obtiverem as maiores pontuações será realizada uma análise de custo, configuração, eficácia e abrangência.

Com os dados serão apresentadas soluções de baixo custo, que irão atender ao principal objetivo da pesquisa, soluções de baixo custo com bom nível de segurança.

1.3 **RELEVÂNCIA**

A relevância deste estudo foi desenvolvida para apresentar como é possível uma Pequena Empresa com baixo orçamento, estruturar um ambiente com um bom nível de segurança.

A pesquisa utiliza dois alicerces para validar a conclusão do trabalho. O primeiro é a coleta de dados de diferentes fontes, com perfis parecidos, profissionais que trabalham com segurança da informação em diferentes Estados do Brasil.

A importância prática desse trabalho se resume na apresentação de soluções de baixo custo, com um alto grau eficiência e uma abrangência considerável.

Do ponto de vista acadêmico, como as soluções apresentadas serão de baixo custo, os softwares recomendados podem ser utilizados para estruturar ambientes que precisem de um bom nível de segurança a baixo custo.

1.4 **ORGANIZAÇÃO DO TRABALHO**

Este projeto está subdividido em três etapas principais:

A primeira visa ilustrar conceitualmente os principais ataques, tecnologias de Firewall [1], o funcionamento dos IDS [3], descrever as principais ameaças de rede, explicar a visão conceitual dos softwares de análise de vulnerabilidade [3].

A segunda etapa visa o desenvolvimento, tem como principal objetivo analisar os dados coletados nas entrevistas, e definir os softwares que serão recomendados especificando-se as fórmulas que foram utilizadas para se chegar a uma conclusão.

Nesta fase da pesquisa, ela será fundamentada nos seguintes parâmetros: Custo, dificuldade de configuração, abrangência e eficácia. Esses softwares

selecionados serão descritos de forma que um administrador de uma pequena empresa poderá escolher qual solução irá atender a necessidade da sua empresa.

A terceira etapa tem por finalidade analisar as informações da etapa anterior, para definir as soluções que atendam ao principal objetivo da pesquisa, ou seja, soluções de baixo custo, com facilidade de configuração, abrangência e eficácia.

2 REFERENCIAL TEÓRICO

2.1 CONSIDERAÇÕES INICIAIS

O capítulo apresenta a fundamentação teórica, de todos os elementos envolvidos no desenvolvimento do trabalho, de forma a fornecer o embasamento teórico para o desenvolvimento do próximo capítulo, onde serão analisados softwares de análise de vulnerabilidade [3], firewalls [1], IDS [3], e percentuais de ataques por categoria.

Todas as soluções analisadas na pesquisa serão indicadas por profissionais que trabalham com segurança da Informação.

2.2 TIPOS DE ATAQUES

Os ataques podem ser iniciados explorando falhas do sistema operacional, atualmente ocorrem diversos tipos de ataques. Alguns são ataques complexos, que são desencadeados por vários computadores ao mesmo tempo, ou em apenas um computador.

Existem ataques que objetivo é coletar informações do sistema analisado, outros têm como objetivo o acesso ao sistema.

Esse ponto da pesquisa explica os principais tipos de ataques para fornecer o embasamento conceitual de diversas formas de ataques. [1] [2] [3] [6] [7]

2.2.1 Ataques de Negação de Serviço

São caracterizados pela paralisação ou lentidão do serviço. O impacto pode ser de minutos ou horas, o principal objetivo desse ataque é a exploração de vulnerabilidades, com o objetivo de saturar a largura da banda da rede, gerando a paralisação de sistemas. Nessa categoria os ataques mais conhecidos são flood e

spoof. O ataque de flooding é muito complicado a detecção, porque a origem do ataque é mascarada, dificultando a identificação do atacante. Os ataques mais freqüentes são os ataques lógicos e os ataques de inundação. Os ataques lógicos utilizam programas de rede, para explorar vulnerabilidades para assim paralisar o serviço. [1]

Os ataques de inundação utilizam um grande envio de pacotes o que acarreta problemas na rede.

Esse tipo de ataque pode utilizar milhares computadores que estejam contaminados por algum tipo de vírus. Esses computadores atacam as vítimas definidas pelo criador do vírus, esse tipo de ataque é chamado de DDOS (Distributed Denial of Service ou DDOS). [2][4]

2.2.2 **Buffer Overflow Attack**

Ocorre quando um processo recebe muitas informações que não eram esperadas.

A rotina de programação não especificou o tamanho máximo do dado, com esse procedimento é possível invadir um sistema.

Existem vários tipos de ataques que utilizam buffer Overflow, um tipo de ataque é o ping da morte, que consiste na utilização de mais de 256 caracteres nome do usuário ou nome do arquivo de e-mail. Para ocorrer esse ataque é gerado um grande pacote de ping, que utiliza pacotes ICMP. O invasor envia o ping modificado com um tamanho de datagrama alterado, o sistema que recebe o ping estoura o buffer e reinicia. [1] [6] [7]

2.2.3 **SYN Attack**

Um ataque SYN ocorre quando um exploit estoura o tamanho do buffer durante a transmissão do TCP. Isso ocorre quando o TCP está iniciando a sessão do Handshake. Após o ataque o sistema fica inoperante. [1] [6]

2.2.4 **Teardrop Attack**

Consiste em modificar o tamanho do fragmento no campo OFFSET do pacote do protocolo IP. O alvo do ataque irá ocorrer um crash após receber informações contraditórias de instruções de como fragmentar OFFSET dos pacotes. [1] [7]

2.2.5 **Smurf**

O ataque se caracteriza pela combinação do ip spoffing e da saturação da rede com trafego.

O ataque utiliza dois elementos, o site de origem e o site destino. O atacante envia pacotes de ping spoofed [1] para todos os endereços de rede. A modificação do pacote consiste no endereço do destino. Todos os dispositivos irão responder a resposta para o destino do sistema que na verdade é outro endereço. Com isso todas as respostas serão direcionadas para esse endereço, o que irá ocorrer à saturação do sistema ou da rede. [3]

2.2.6 **Corrida contra o tempo**

Essa falha funciona como se fosse uma corrida contra o tempo. Quando algum usuário comum cria um arquivo com permissão de usuário administrativo ou superusuário [2], essa permissão é finita dura no máximo alguns segundos, antes de ser apagada.

Com essas permissões elevadas podem aumentar o privilégio de um usuário dentro de um sistema [2], são utilizados programas geradores de loop, para que o

processamento da maquina fique mais lento, disponibilizando alguns segundos para as modificações necessárias. [2]

2.2.7 **SQL Injection**

Atualmente é considerado um dos principais ataques utilizados. Utiliza comandos de SQL exploram a interação com o banco. Funciona com linguagens diferentes PHP, ASP, JSP entre outras [2]. O programador quando desenvolveu, não interpretou certos caracteres como (/) e aspas simples (´) que poderão ser utilizadas, para colocar comandos no sistema, neutralizando os sistemas de login e senha, fornecendo acesso completo ao banco de dados quantas vezes forem necessárias. [3]

2.2.8 **PHP Injection**

Funciona de forma muito parecida com o SQL Injection, um script malfeito, que não trata sua entrada de dados ou cria links corretamente e abre portas que podem ser invadidas. [2]

2.2.9 **Cross Site Scripting**

Também conhecida como CSS ou XSS, o Cross Site tem como objetivo roubar cookies de usuário através de seus navegadores. O ataque utiliza comandos HTML e Java Script, o invasor consegue obter sessões de usuários sem permissão do mesmo. Para se ter uma idéia da sua utilidade com essa técnica, poderia ler o e-mail de uma pessoa no Webmail sem ter conhecimento da senha. [2]

2.2.10 **Engenharia Social**

O principal objetivo da Engenharia Social é coletar informações importantes de uma pessoa, funcionário, empresa. Essa técnica pode ser dividida em dois grupos pesquisa e falsidade ideológica.

A pesquisa procura informações no lixo, realiza contatos com outras pessoas, utiliza vários meios que possam servir para descobrir as informações procuradas [1]. A falsidade ideológica tem relação direta com o disfarce, ilusão. Essa técnica é considerada umas das mais difíceis de combater, uma vez que tem envolvido o elemento “humano” e sua capacidade de armazenamento de informação, e muitas vezes é o único envolvido não fazendo uso de tecnologia. [3]

2.2.11 **Analisadores de Portas “PortScanners”**

São softwares que tem como principal objetivo, analisar quais portas estão disponíveis no equipamento analisado. Esse software consegue levantar todas as portas que estão abertas, quais serviços estão ativos, e como os serviços são definidos em portas diferentes, é possível identificar quais softwares estão instalados. O software consegue

Informações importantes sobre os sistemas analisados. O principal portscanner utilizado no mercado é o Nmap.

2.2.12 **Ataques de Botnets**

O ataque é caracterizado, pela utilização de redes zumbis que são formadas por computadores que tiveram códigos maliciosos instalados.

Os computadores, são utilizados para serem gerenciados remotamentes pelos atacantes, formando assim redes que são chamadas de Botnets. Essa redes são utilizadas para atacar servidores derrubando sites, invadindo sistemas, além disso são utilizadas para enviar spam. Esse tipo de ataque dificulta a decoberta do verdadeiro atacante.

2.2.13 **Spoofing de Arp**

Consiste em uma técnica que modifica o Cache de ARP. O cache contém informações do mapeamento endereço MAC para o endereço IP. O ataque se baseia em utilizar mesmo endereço MAC [3], mas o atacante assume o endereço IP do computador confiável, depois de assumir o endereço IP são enviadas informações para o alvo do ataque e para o cache.

Nesse momento, os pacotes do alvo do ataque serão roteados, para o seu endereço de Hardware. [3]

2.2.14 **DNS Spoofing**

Funciona da seguinte forma, o tráfego da rede é interceptado, são utilizadas respostas falsas para as requisições DNS dos clientes [2].

As requisições podem ser de várias formas A PTR qualquer registro. Todas as informações serão alteradas de acordo com as necessidades dos atacantes. [2]

Quando o atacado tentar se conectar em um site www.teste.com.br ele será enviado pra outro site que o atacante definiu.

2.2.15 **Zero day Vulnerabilities**

Consiste na exploração de uma vulnerabilidade que foi divulgada no mesmo dia, por serem muito recentes pode não existir ainda uma solução do fabricante.

Atualmente a maioria das vulnerabilidades é notificada para os fabricantes antes de serem divulgadas, para os fabricantes realizarem as modificações necessárias.

Caso essa vulnerabilidade, não tenha sido resolvida pelo alvo do ataque.
O atacante aproveita esse tempo, entre a aplicação da correção, para tentar explorar essa vulnerabilidade.

2.3 DESCRIÇÃO DAS PRINCIPAIS TECNOLOGIAS DE FIREWALLS

Atualmente no mercado as maiorias dos softwares utilizados, operam na camada de transporte e de rede do modelo TCP/IP [1], tendo como principal utilização a filtragem de pacotes.

São analisados todos os pacotes que entram ou saem das interfaces de rede a ele conectadas, ou seja, analisam tanto pacotes destinados diretamente ao Firewall, quanto àqueles destinados a qualquer computador conectado a ele por meio de alguma de suas interfaces de rede [11]. Sua principal função também é bloquear todas as portas quem não estejam sendo utilizadas.

Existem várias gerações, segue abaixo em ordem as várias gerações que foram desenvolvidas.

2.3.1 Filtro de Pacotes Estáticos

O primeiro tipo de firewall que examina pacotes, ele funciona examinando a origem e o destino dos pacotes.

Esse software consegue bloquear ou liberar pacotes para a rede de destino que normalmente é a rede local onde ele está situado. Tem a capacidade de bloquear acesso a determinadas aplicações ou serviços, utilizando listas de controle de acesso (ACLS) [11] onde o seu arquivo de configuração reside no próprio equipamento [1]. A configuração é definida e gerenciada pelo administrador.

O firewall pode ser configurado para liberar acesso a aplicações que operam com determinadas portas especificas [1].

O filtro de pacotes analisa os pacotes de dados, verifica informações sobre origem e destino para poder encaminhar os dados, podem ser configurados vários protocolos, (TCP, UDP, ICMP) [7] e portas de determinados serviços ou aplicativos.

Essa geração é considerada a primeira geração, podendo operar na camada de rede ou transporte do modelo OSI. [1] [3] [11]

2.3.2 **Nível de Aplicação**

Opera transferindo cópias de pacotes de dados aceitos em uma rede para outra rede, mascarando os dados originais é conhecido com servidor Proxy.

Consegue controlar quais serviços serão usados pelas estações (FTP somente), além disso, conseguem proteger a rede interna de tentativas de levantamento de informações sobre a rede local. [1]

Este aplicativo é considerado a segunda geração, operando no modelo no nível sete, camada de aplicação. Reduz o rendimento da rede, mais pode analisar todos os pacotes e decidir quais pacotes serão aceitos [1]. São chamados de nível de circuito, porque conseguem criar circuitos virtuais entre as estações e o servidor. Com esse mecanismo melhora a segurança para vários protocolos, além da facilidade de manutenção. [1] [3] [11]

2.3.3 **Estado de Conteúdo**

O Firewal que utiliza estado de conteúdo tem a capacidade de analisar pacotes de dados capturados rapidamente na camada de aplicação. [1]

Os pacotes são analisados por todas as camadas do modelo OSI. Esse equipamento consegue uma melhor performance, comparando com firewall em nível de aplicação, a grande vantagem que é possível uma analise completa dos dados. Analisando o estado o conteúdo dos pacotes recebidos, isso ajuda os protocolos que são considerados de conexões, como o UDP ou RPC. Esse tipo de firewall é considerado a terceira geração. [1] [3] [11]

2.3.4 **Filtro de Pacotes Dinâmico**

Essa é a quarta geração, porque habilita a modificação das regras de segurança. É utilizada para providenciar limites no UDP. [1]

Funcionam da seguinte forma, por um pequeno período de tempo, armazenam todos os pacotes UDP que passam no perímetro da rede, assim tem a capacidade de decidir quais pacotes poderão passar conseguindo dinamismo e perfomace. .[1] [3] [11]

2.3.5 **Kernel Proxy**

Kernel Proxy [1] foi considerada a quinta geração, porque providencia módulos baseados no kernel, múltiplas camadas de sessão podem rodar simultaneamente. A arquitetura que esse firewall utiliza, pode dinamicamente customizar pacotes TCP/IP, inspecionando na rede e configurando políticas de segurança. [1] [3] [11]

2.4 ARQUITETURAS DE FIREWALL

2.4.1 **Screening Router**

Essa arquitetura foi desenvolvida para trabalhar com dispositivo que tem como funcionalidade filtrar e rotear pacotes, objetivo principal dessa arquitetura é defender o perímetro da rede interna. O roteador tem que ser configurado com regras bem definidas para proteger de forma segura a rede interna da Internet. .[1] [3] [11]

2.4.2 **Dual-hommed Host**

Essa arquitetura opera com um único dispositivo, a conexão opera com duas conexões a primeira com o firewall e a segunda com a conexão de destino. Não é realizado roteamento de pacotes, ele atua como servidor Proxy. [1] [3] [11]

2.4.3 **Screened Host**

Ele tem como função bastion host, que funciona como roteador e filtro de pacotes. Todos os pacotes que não tem como destino o próprio bastion host serão descartados. Ele tem uma função importante de Proxy, que bloqueia o acesso da rede interna para Internet. O maior problema dessa arquitetura é a fragilidade de um ponto único de falha, se o servidor for invadido terá acesso à rede interna sem maiores problemas. .[1] [3] [11]

2.4.4 **Screened Subnet (DMZ)**

Essa arquitetura é considerada a mais segura das arquiteturas, tem como principal objetivo a criação de perímetros em uma zona desmilitarizada.

É utilizado um Bastion Host que fica localizado dentro da DMZ. A comunicação é feita através desse bastion host, que estabelece uma conexão entre a estação e o bastion host, protegendo a rede interna da internet.

Essa arquitetura utiliza dois roteadores um roteador interno, e outro externo. Por isso é incrementada uma camada adicional de proteção da rede interna. .[1] [3] [11]

2.5 **DESCRIÇÃO DO FUNCIONAMENTO DOS IDS**

Os IDS são desenvolvidos para reconhecer ataques e modificações na rede. Quando ocorre alguma modificação no comportamento do tráfego, ou a caracterização de algum ataque [3] é enviada alerta para os administradores contra-atacar ou para se defender, utilizando alguma tecnologia de defesa. Atualmente a maioria dos sistemas de detecção de invasão tem como principal objetivo, procurar possíveis invasores. [12] [13]

Os IDS na maioria dos sistemas são utilizados em três tipos: modelo de detecção de mau uso e modelo de detecção baseado em anomalia. O modelo de detecção de

mau uso divide-se em dois modelos: sistemas de detecção baseados em rede (NIDS) e sistemas baseados em host (HIDS) [3]. Os mais modernos utilizam a tecnologia (HIPS) [14]. Segue abaixo a descrição desses modelos: [3] [12] [13]

- **IDS baseado em rede** - Os NIDS analisam os pacotes como sniffers. Eles capturam o tráfego, e analisam com um conjunto de padrões de ataques ou assinaturas. Essa comparação nos pacotes identifica possíveis invasores. Eles são desenvolvidos para inspecionar o tráfego de rede, e procurar padrões de ataques ou assinaturas, essa tarefa é feito com uma placa de rede em modo promíscuo para a análise dos frames. Atualmente os IDS utilizam atualização das assinaturas, para tentar manter as assinaturas atualizadas para detectar novos tipos de ataques. Um dos problemas do NIDS é suportar a alta capacidade da banda das redes analisadas, o que pode corromper ou paralisar seu funcionamento. [3][12][13]
- **IDS baseado em host** – Esse tipo de IDS opera analisando logs dos sistemas. Para o funcionamento são necessários agentes em cada ambiente analisado. Esse tipo de IDS gera um grande esforço administrativo para instalação dos agentes. Em compensação a análise é mais intrusiva, por causa do agente ser instalado no próprio sistema facilitando a análise. [3]
- **IDS baseado em anomalia** – O funcionamento desse tipo de IDS (NIPS) [14] é diferente dos outros, porque este é reativo, quando detecta algum um tipo de anomalia especifica em alguma assinatura ou alerta, o pacote é automaticamente bloqueado, diferenciando bruscamente dos antigos IDS, que só alertavam o problema. O NIPS é baseado na proteção do conteúdo dos pacotes, tentam proteger a rede, de forma mais eficiente do que os antigos IDS. Recentemente certos IPS bloqueiam pacotes utilizando os

mesmos critérios dos Firewalls chegando a ser agregados em soluções fechadas de firewall. [3] [14]

2.5.1 Informações Importantes para Analisar um IDS

Para definir qual IDS será utilizado, é necessário avaliar três pontos fundamentais, o tráfego na rede que será analisado, as características do produto, e a atualização.

Os IDS são dependentes de atualizações, se não ocorrer á atualização o sistema irá ficar inoperante com o tempo, por isso é fundamental a atualização regular. Existem várias diferenças entre fornecedores diferentes, é fundamental verificar os recursos básicos e os acessórios desses produtos. Segue abaixo uma lista de itens que podem ajudar a escolha do IDS: [3]

- **Profundidade de cobertura** – Um dos principais pontos de um IDS é a capacidade de detectar o maior número de ataques. Verifique se a solução de NIDS analisada contempla um grande número de assinaturas de ataques, é fundamental que ela seja compatível com as plataformas que você precisa monitorar [3].
- **Precisão de cobertura** – É difícil determinar sem teste completo, as assinaturas que não foram criadas iguais. As soluções com NIDS apresentam um grande número de falso-positivos, e em grandes quantidades podem colocar em risco a eficácia do IDS. Atualmente existem produtos que conseguem reduzir a quantidade de falso-positivos [3].
- **Arquitetura** – Tem que ser projetada para ser robusta, suportar técnicas básicas tanto de ataque como de evasão. Problemas de evasões nos

dispositivos de NIDS reduzem a eficácia dos produtos e a confiança dos analistas de segurança [3].

- **Escalabilidade** – Os dois maiores problemas são a monitoração de grandes larguras de banda, e o gerenciamento dos dados. Existem NIDS que tem dificuldades de monitorar altas larguras de banda. Por isso os fabricantes desenvolveram hardwares específicos para suportar altas capacidades de banda [3].
- **Estrutura de gerenciamento** – Para dinamizar o funcionamento do IDS, é necessária a apresentação dos dados coletados. Os administradores podem acessar os dados e visualizar os ataques. A estrutura de gerenciamento é fundamental para uma boa administração [3].
- **Atualizações** – Para um perfeito funcionamento, é necessário que sejam criadas atualizações regularmente, assim o IDS estará sempre atualizado identificar novos ataques [3].
- **Personalização** - Alguns produtos permitem várias personalizações, enquanto outros não permitem. Quando escolher um fornecedor é interessante escolher suas necessidades atuais como as do futuro [3].
- **Requisitos de operação** – Esses dispositivos devem ser tratados por pessoas treinadas com alta qualificação [3].
- **Reatividade** – Verificar se existe soluções de IPS para o IDS analisado [14] [3]

2.6 **SCANNERS**

Os scanners são divididos em três categorias:

2.6.1 **Scanners de Vulnerabilidades**

Esse pacote de software é utilizado para analisar a configuração de hosts especificados. São analisadas várias características do host falhas no sistema operacional, portas abertas, vulnerabilidades de vários tipos.

Alguns softwares chegam a realizar tentativas de invasão para explorar essas vulnerabilidades que foram detectadas.

Esse tipo de software tem uma característica de conhecer vários tipos de vulnerabilidades, por isso são muito utilizados na verificação de segurança de novos computadores e na analise de vulnerabilidades de sistemas em produção, realizando a auditoria dos sistemas, porque além de indicar as vulnerabilidades, geram recomendações para solucionar os problemas identificados.

2.6.2 **Scanner de Rede**

São utilizados para realizar varreduras na rede, detectando computadores remotos que estejam vulneráveis a ataques. Com esse tipo de mapeamento das portas tanto um analista de segurança como um invasor pode realizar o mapeamento das portas que estão abertas e fechadas.

Por isso esses softwares são utilizados por analistas de segurança, para realizar auditorias de segurança como invasores, que desejam invadir os sistemas.

2.6.3 **Scanner de Host:**

Esse tipo de scanner tem como característica, que o software que irá realizar a auditoria do computador, está instalado no próprio, o que facilita o levantamento de

informações cruciais do sistema analisado. São verificadas várias configurações, processos executados, permissões, softwares instalados, compartilhamento de rede, hardware instalados, além de outras configurações. A grande desvantagem é o esforço administrativo de ter que instalar um agente em cada computador analisado.

2.7 PRINCIPAIS AMEAÇAS DE REDE

As principais ameaças de uma rede estão divididas em duas categorias:

- Ataques, internos
- Ataques externos

2.7.1 **Ataques Internos**

Esse tipo de ataque ocorre constantemente, estatisticamente com um número maior de ataques em redes internas, do que explorações remotas bem-sucedidas em redes remotas. A grande vantagem do atacante, que ele tem acesso á rede interna ou a estrutura física da Empresa, facilitando acesso a informações. Além de informações de sistemas da rede interna, o que facilita o acesso.

Os administradores têm grande dificuldade em reconhecer esse tipo de ataque, porque ficam muito preocupados com ataques externos, e normalmente não é implementada a proteção interna eficiente, o que acaba facilitando esse tipo de ataque. [3] [6] [7]

2.7.2 **Ataques Externos**

A característica do ataque externo tem origem externa ao perímetro interno. Existem vários tipos de ataques externos, negação de serviço, vírus, modificações em páginas Web, cavalo de tróia, worms entre outros.

Atualmente existem vários tipos de equipamentos que podem ser utilizados pelas Empresas para minimizar os riscos associados a esse tipo de ataque.

Normalmente esses ataques ocorrem contra serviços, sistemas e redes acessíveis. A melhor proteção contra esse tipo de ataque externo é o uso de um firewall que tenha integrado em seu hardware, uma solução de antivírus, anti-spam e IPS. [1][2] [14]

3 METODOLOGIAS DE PESQUISA [1]

3.1 **INTRODUÇÃO**

Neste capítulo, abordaremos o tipo de pesquisa que guiará a aplicação desta investigação. Depois será apresentando o modelo de referência, que será utilizado como embasamento da pesquisa, e as hipóteses para solucionar ajudar a solucionar o problema pesquisado.

Alem disso, será definido o universo do problema, as amostras que serão utilizadas para demonstrar aonde as pesquisa serão aplicadas.

Para concluir o capitulo serão apresentados às fases da coleta de dados, a análise e interpretação desses dados, e após ser feito essa análise, serão descritos as limitações do método de pesquisa utilizado.

3.2 **TIPO DE PESQUISA**

O paradigma que será usado na pesquisa é o mixed, que utiliza informações coletadas em uma pesquisa quantitativa, que tem como objetivo coletar informações de um grupo de profissionais que trabalham com segurança da informação. Essas informações serão coletadas com questionários, que serão analisados e transformados em números, para análises estatísticas. Após essa análise os dados serão apresentados em gráficos com percentuais.

Além das informações coletadas na pesquisa quantitativa, baseando-se no paradigma quantitativo, serão realizadas análises qualitativas das respostas dos entrevistados, para interpretar a opinião dos entrevistados com informações coletadas em bibliografias e documentos teóricos.

---

[1] Esse capítulo utilizou como embasamento teórico a referência [15]

O paradigma de pesquisa utilizado será quantitativo, para aprofundar opiniões de profissionais de segurança, sobre questões objetivas para assim ajudar Pequenas Empresas, com baixo orçamento a manter um bom nível de segurança. Utilizaremos como método o *survey*, não apenas por ser adequado à pergunta do estudo, mas principalmente a contribuição que esse método pode ajudar a indicações sobre questões objetivas, a fim de possibilitar a comparação dos resultados.

Esta pesquisa será exploratória, porque irá coletar informações de profissionais de diferentes regiões do País, e será também descritiva e explicativa, visando expor as características do fenômeno para definir possíveis soluções, contribuindo para uma solução eficaz para a necessidade do problema.

Os meios utilizados, serão a pesquisa de campo (*survey*), pesquisas na Internet, bibliografias (livros, revistas, etc). Todos esses meios tem como finalidade ajudar ao embasamento teórico e pratico da pesquisa.

O método *survey* que será utilizado será baseado em um questionário preparado com perguntas abertas e fechadas para dinamizar as respostas.

Com as perguntas fechadas serão feito estatísticas, nas perguntas abertas serão utilizadas para análise para ajudar a conclusão com embasamento teórico e prático. Este *survey* será aplicado em uma amostra de profissionais de várias cidades que trabalham com segurança da Informação a fim de verificar as recomendações desses profissionais.

3.3 **MODELO DE REFERÊNCIA DA PESQUISA**

Esta pesquisa tem como objetivo explicar como Pequenas Empresas com baixos orçamentos, podem estruturar um bom nível de segurança.

O referencial foi desenvolvido para estruturar o embasamento teórico para o desenvolvimento da pesquisa. Como serão analisados vários softwares de segurança, que serão definidos após a coleta de dados na pesquisa, foi necessário explicar o funcionamento de algumas tecnologias que fazem parte da pesquisa. Gerando o embasamento teórico que precisamos entender para o pleno funcionamento dessas tecnologias.

Como serão analisados o funcionamento a eficácia e a abrangência desses softwares, que são fundamentais para manter uma estrutura com bom nível de segurança. Foi necessária a explicação teórica das tecnologias analisadas (Firewall, IDS, Scanner de Análise Vulnerabilidade) além dessas tecnologias foi necessário explicar outras tecnologias como técnicas de ataques, ameaças de rede.

3.4 **HIPÓTESES**

Buscaremos, neste estudo, estruturar soluções de segurança que ajudem a contemplar soluções de segurança para Pequena Empresa com baixo orçamento, por isso serão levantados dados via coleta de dados, com profissionais que trabalham com segurança da informação.

Esses dados coletados, vão ter informações sobre recomendações sobre algumas categorias de softwares, definindo a dificuldade de configuração, eficácia e abrangência.

Além dessas recomendações serão coletadas, informações sobre quais ataques essas Empresas estão mais sujeitas a sofrer.

Com esses dados coletados, será realizado um estudo sobre os principais softwares recomendados na pesquisa. Esse estudo terá como base o custo, dificuldade de configuração, abrangência e eficácia, para desta forma recomendar uma solução que consiga abranger o objetivo da pesquisa.

3.5 **UNIVERSO E AMOSTRA**

O universo será composto por profissionais de grande experiência, que trabalham com segurança da Informação, em diferentes estados Brasileiros. Esses profissionais estão alocados nas cidades do Rio de Janeiro, São Paulo, Fortaleza e Recife. Com experiência em vários projetos, esses profissionais, que em média tem mais de trinta anos, podem ajudar com recomendações, para solucionar o problema pesquisado.

A amostra será composta pela resposta desses profissionais, apresentação da amostra será estruturada, de acordo com as respostas que o pesquisador encontrar, por isso são fundamentais para pesquisa.

Como objeto de estudo da pesquisa é definir como uma Pequena Empresa com baixo orçamento consegue estruturar um bom nível de segurança, serão coletadas informações com profissionais altamente qualificados, para realizar uma amostragem probabilística casual simples para determinadas questões, e estratificada para outras questões.

Além desses dois itens serão apresentadas de forma não probabilística acidental, questões que apresentam diferentes visões de um determinado assunto.

3.6 **COLETA DE DADOS**

A coleta de dados será realizada inicialmente utilizando a metodologia de coleta de dados primária. As informações coletadas serão do universo especificado no item anterior.

Serão realizadas entrevistas estruturadas por telefone, utilizando um questionário com perguntas abertas e fechadas para dinamizar as respostas dos entrevistados. A grande vantagem das perguntas fechadas é conseguir uma padronização das respostas com certa uniformidade, o que facilita a demonstração dos resultados utilizando gráficos.

Entretanto as perguntas que forem elaboradas abertas conseguem uma maior abrangência das respostas, o que facilita o aprofundamento do fenômeno analisado ou de novas descobertas que ainda não foram analisadas.

Após concluir a coleta de dados primária, será realizada uma coleta de dados secundária para analisar os custos das soluções.

Os principais itens que foram identificados na coleta primária serão analisados para assim chegar a uma conclusão que terá como base a experiência dos profissionais entrevistados, embasamento teórico e o custo dos itens analisados.

3.7 **ANÁLISE E INTERPRETAÇÃO DOS DADOS**

Após a coleta de dados primária, será feito uma análise e uma interpretação dos dados coletados. Nas perguntas abertas será utilizado o modelo qualitativo, aonde serão definidas categorias para tabular, e estabelecer relações. Nas perguntas fechadas serão utilizados o modelo quantitativo para tratar dados estatísticos, contagem de resultados e estabelecimento de relações.

Após análise dos dados coletados, será realizada uma coleta de dados secundária, para ajudar no embasamento teórico dos softwares que tiverem alto percentual de indicação pelos profissionais entrevistados, serão analisadas facilidade de configuração, custo, abrangência e eficiência.

3.8 **LIMITAÇÕES DO MÉTODO** [2]

Como o método escolhido foi o método survey, a coleta de dados foi muito difícil, porque como o foco das entrevistas, eram profissionais que trabalham com segurança da Informação, existe uma grande resistência desses profissionais em fornecer informações. Tanto que determinadas Empresas de Segurança somente permitem que algum funcionário forneça algum tipo de entrevista se tiver autorização da Empresa o que acaba dificultando a coleta de dados..

As entrevistas que realizei, a maioria foi por intermédio de contatos profissionais, se não fossem esses contatos as barreiras seriam ainda maiores.

Com relação às entrevistas foram proveitosas, conseguindo informações muito importantes, que irão ajudar a obter os resultados pretendidos dentro do universo estudado.

---

[2] A coleta de dados foi realizada somente com profissionais que trabalham com Segurança da Informação.

4 RESULTADOS

4.1 ANÁLISE DESCRITIVA DA AMOSTRA [3]

Os entrevistados que responderam as perguntas, tinham o mesmo perfil, todos trabalham com segurança da Informação, mas com cargos diferenciados, o que contribui alguns assuntos, dando um aprofundamento sobre determinado temas.

O item fundamental para a escolha dos entrevistados, era experiência profissional, embasamento teórico, trabalhar com segurança, tanto que a idade média dos entrevistados ficou em 30 anos.

Para oferecer uma maior contribuição para a pesquisa, foram coletadas informações de profissionais de diferentes regiões, centralizando nas cidades do Rio de Janeiro, São Paulo, Recife e Fortaleza.

Segue abaixo o perfil dos entrevistados:

- Diretor Executivo responsável pela área tecnológica da Empresa
- Diretor responsável pela área de Segurança
- Gerente de Segurança
- Consultor Sênior de segurança
- Analista de segurança Sênior
- Engenheiro de Sistemas com ênfase no desenvolvimento de softwares de segurança
- Analista de Infra-estrutura e segurança Sênior

[3] As informações com as idades dos entrevistados, foram retiradas dos questionários respondidos.

Segue abaixo um gráfico com a Idade dos Entrevistados. A média ficou em 30,4.

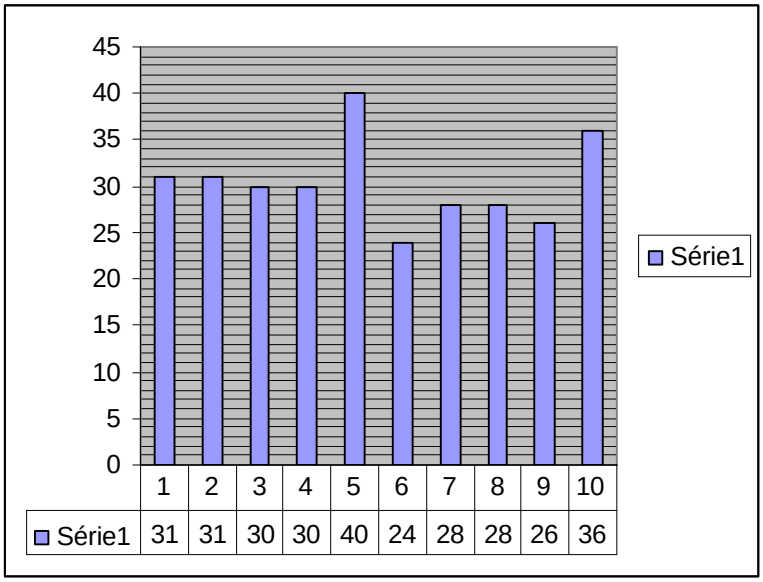

Ilustração 1–Gráfico com as idades dos entrevistados

4.2 ANÁLISE DOS ITENS DO QUESTIONÁRIO

O questionário foi desenvolvido com o objetivo de coletar informações primárias dos entrevistados, foram desenvolvidas nove questões.

As quatro primeiras questões tinham como objetivo, coletar informações diferenciadas sobre quatro categorias de software.

A primeira questão foi desenvolvida com objetivo de coletar as indicações de cada profissional.

A segunda questão tinha como objetivo definir a dificuldade de configuração de cada software indicado.

A terceira questão tinha como objetivo coletar informações sobre a eficiência desses softwares.

A quarta questão seguiu a mesma linha de raciocínio das outras questões, sendo que a informação coletada seria a abrangência.

Após o término da coleta foi desenvolvida uma planilha para pontuar os softwares em cada categoria, definindo as pontuações e classificação.

Foram desenvolvidas fórmulas para pontuar os softwares, utilizando diferentes parâmetros com pontuações diferenciadas. Os parâmetros indicação e eficácia tiveram maiores influência no resultado final.

Como as informações coletadas foram de extrema importância para a pesquisa. As indicações dos entrevistados teriam que ter um peso maior na pontuação final, outro parâmetro que teve um valor diferenciado foi à eficácia, porque esse parâmetro é de extrema importância para a definição de qualquer solução.

As informações que estão nas tabelas abaixo foram retiradas dos questionários.

Em cada parâmetro foi somado o total de respostas iguais, e colocados em uma tabela, totalizando um total por item respondido. Após esses dados serem colocados nessa tabela foram aplicadas fórmulas para pontuar os softwares.

Após aplicação das fórmulas é definida a pontuação e as classificações das soluções analisadas.

A fórmula desenvolvida utiliza todos os parâmetros analisados, indicações, dificuldade de configuração, eficácia e abrangência.

Segue abaixo como exemplo, a tabela da categoria firewall, estão detalhadas os valores totais em cada parâmetro:

Quadro 1 – Total de indicações na categoria Firewall

Firewall	Ind.	Dififuldade	Eficácia	Abrangência
Iptables	7	D=3 /M=3/F=1	E=1/B=5/Ra=1/M=0/R=0	C=1/In=2/R=4
Check Point Safe@Office 500	7	D=0/M=2/F=5	E=5/B=1/Ra=1/M=0/R=0	C=7/In=0/R=0
Sonic Wall tz 190	4	D=0/M=1/F=3	E=0/B=4/Ra=0/M=0/R=0	C=3/In=0/R=1
PF	1	D=1/M=0/F=0	E=1/B=0/Ra=0/M=0/R=0	C=1/In=0/R=0
ISA Server	3	D=0/M=3/F=0	E=1/B=1/Ra=1/M=0/R=0	C=1/In=2/R=0
Shorewall	1	D=0/M=0/F=1	E=0/B=1/Ra=0/M=0/R=0	C=0/In=0/R=1
Check Point UTM - 1 Edge	5	D=0/M=4/F=1	E=4/B=1/Ra=0/M=0/R=0	C=4/In=1/R=0
Firewall Builder	1	D=0/M=1/F=0	E=1/B=0/Ra=0/M=0/R=0	C=1/In=0/R=0
Cisco Asa	1	D=1/M=0/F=0	E=1/B=0/Ra=0/M=0/R=0	C=0/In=1/R=0

Segue abaixo o significado de cada letra na tabela acima: [4]

D=Difícil/Médio/F=Fácil/E=Exelente/B=Bom/Ra=Razoável/R=Ruim/C=Completa/In=Incompleta

As informações contidas da tabela 1 serão aplicadas às fórmulas descritas abaixo, com os parâmetros e as pontuações em cada item:

- Fórmula para calcular o parâmetro indicação:

Equação 1 = (Formula_Ind) = Cada indicação recebe 1 ponto

[4] Os dados incluídos no quadro 1 foram retirados dos questionários respondidos

Obs: Objetivo desse parâmetro foi atribuir um ponto para cada indicação, totalizando o número total de indicações.

- Fórmula para calcular o parâmetro Dificuldade:

Equação 2 = (Fórmula_Dif) = (F*3+M*2+D*1)

Obs.: Objetivo foi atribuir a maior pontuação as soluções que forem indicadas no item Fácil, porque como o parâmetro analisado é dificuldade de configuração, os softwares que receberem essa indicação têm que receber a maior pontuação.

- Fórmula para calcular o parâmetro Eficácia:

Equação 3 = (Fórmula_Efic) = (E*5+B*4+M*3+Ra*2+R*1)

Obs.: Essa fórmula foi desenvolvida priorizando um peso maior do que outros itens, o motivo foi tentar coletar informações adicionais sobre esse parâmetro e atribuir um peso maior pela sua importância.

- Fórmula para calcular o parâmetro Abrangência:

Equação 4 (Fórmula_Abr) = (C*3+Im*2+R*1)

Obs.: A maior pontuação foi atribuída às soluções que receberam a indicação de abrangência completa.

- Fórmula para calcular o resultado final:

Equação 5 = (Fórmula_Fin) = (Fórmula_Ind + Fórmula_Dif + Fórmula_Efic + Fórmula_Abr)

Obs.: Essa fórmula teve como objetivo somar a pontuação de todos os parâmetros analisados, e indicar as soluções que tiveram as maiores pontuações.

Regra para casos de empate na total de pontos: Caso ocorra empate o vencedor será o que tiver menos indicações, porque conseguiu uma maior pontuação no somatório dos outros parâmetros analisados.

Depois de aplicar as fórmulas descritas no item anterior segue abaixo o resultado da categoria Firewall:

Quadro 2 – Total de pontos com a classificação da categoria Firewall

Firewall	Ind.	Dificuldade	Eficácia	Abrangência	Total
Check Point Safe@Office 500	7	19	32	21	79
Iptables	7	12	28	11	58
Check Point UTM - 1 Edge	5	11	24	14	54
Sonic Wall tz 190	4	11	16	10	41
ISA Server	3	6	12	7	28
PF	1	1	5	3	10
Firewall Builder	1	1	5	3	10
Shorewall	1	3	4	1	9
Cisco Asa	1	1	5	2	9

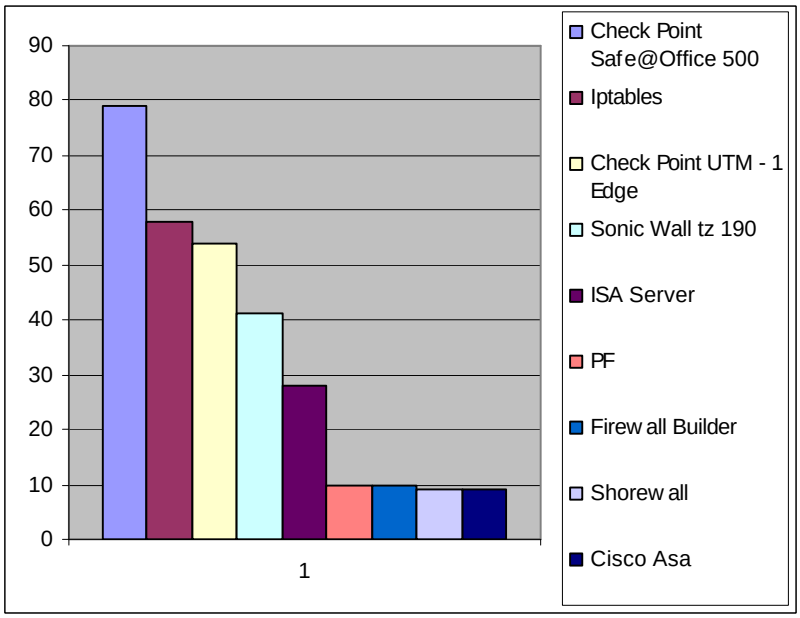

Ilustração 2 - Gráfico com os resultados obtidos na categoria Firewall

Na categoria Scanner de Vulnerabilidades, foram utilizadas as mesmas fórmulas descritas anteriormente, a diferença que os softwares analisados nessa categoria são diferentes.

Segue abaixo a tabela com os resultados obtidos com o total de pontos após a aplicação das fórmulas:

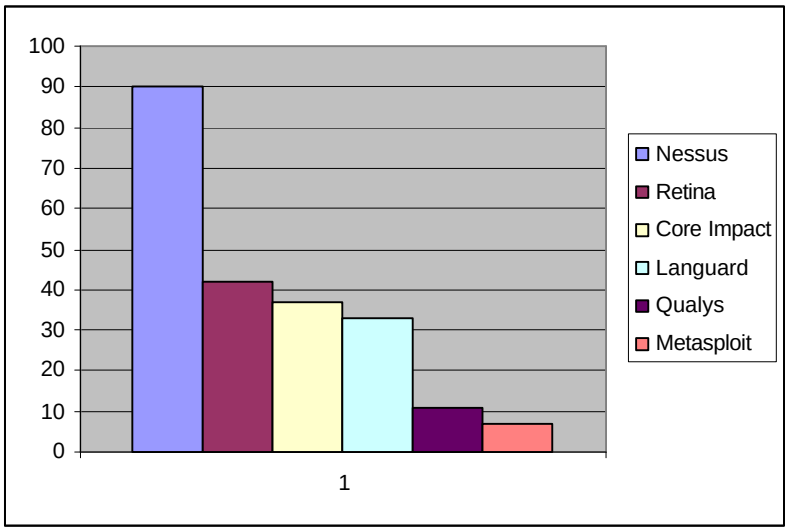

Ilustração 3-Gráfico com os resultados obtidos na categoria Scanner de Vulnerabilidade

Quadro 3 - Total de pontos com a classificação dos Scanners de Vulnerabilidades

Scanner de Vul.	Ind.	Dificuldade	Eficácia	Abrangência	Total
Nessus	9	19	39	23	90
Retina	4	10	17	11	42
Core Impact	4	8	14	11	37
Languard	4	10	10	9	33
Qualys	1	2	5	3	11
Metasploit	1	1	3	2	7

Outra categoria pesquisada foi a dos Scanners de Vulnerabilidade Web, as fórmulas utilizadas foram as mesmas descritas nos itens anteriores, a diferença que os softwares analisados são diferentes.

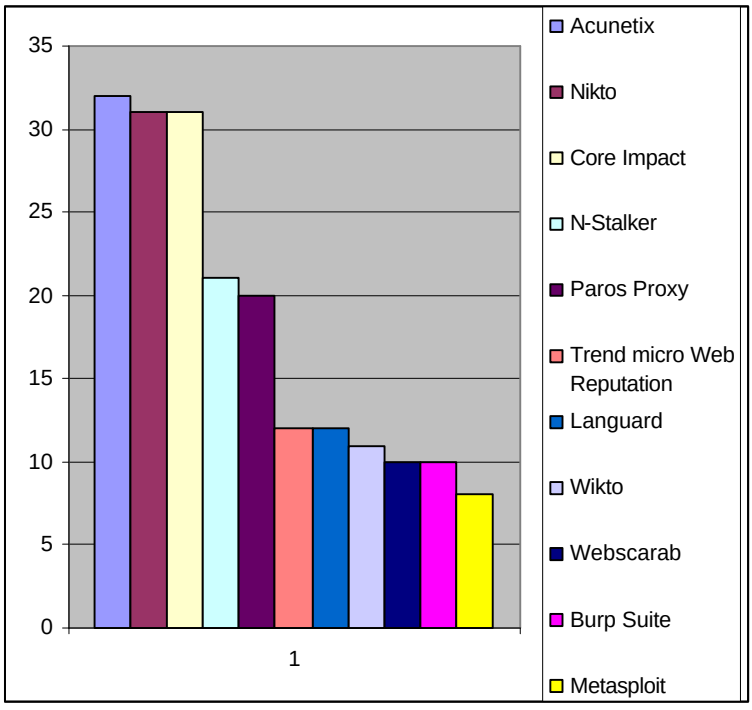

Ilustração 4-Gráfico com os resultados obtidos na categoria Scanner de Vulnerabilidade Web

Segue abaixo a tabela com os resultados obtidos:

Quadro 4 - Total de pontos com a classificação dos Scanners de Vulnerabilidades Web

Scanner de Vuln. Web	Ind.	Dificuldade	Eficácia	Abrangência	Total
Acunetix	3	8	14	7	32
Nikto	4	8	10	9	31
Core Impact	3	8	14	6	31
N-Stalker	2	5	8	6	21
Paros Proxy	2	5	7	6	20
Trend micro Web Reputation	1	3	5	3	12
Languard	1	3	5	3	12
Wikto	1	3	4	3	11
Webscarab	1	3	3	3	10
Burp Suíte	1	3	4	2	10
Metasploit	2	2	2	2	8

Na categoria IDS foram utilizadas as mesmas fórmulas que foram descritas nos itens anteriores, a diferença que as soluções analisadas são diferentes.

Segue abaixo a tabela com os resultados obtidos:

Quadro 5 - Total de pontos com a classificação dos IDS

IDS- Intrusion detect systems	Ind.	Dificuldade	Eficácia	Abrangência	Total
Snort	6	10	25	15	56
Check Point IPS -1	3	5	15	9	32
Source Fire	3	5	13	7	28
Ral Secure	3	4	9	6	22
Mcafee Intrushield	2	4	10	4	20
Cisco Asa	2	4	8	4	18
Shocki	1	2	4	3	10
Shadow	1	2	4	3	10
Ossec	1	1	5	3	10
Cyclops Intrushield	1	2	4	2	9
Check Point Safe@Office	1	1	5	2	9

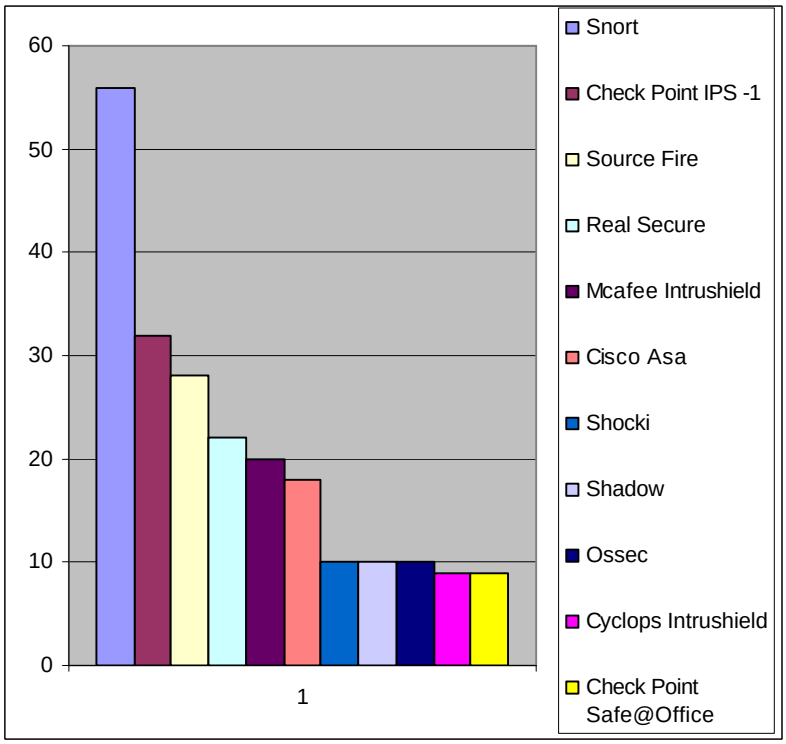

Ilustração 5-Gráfico com os resultados obtidos na categoria IDS

A quinta questão foi desenvolvida com objetivo de coletar informações percentuais dos tipos de ataques que essas Empresas estão mais sujeitas a receber.

Foram definidas cinco categorias, para se chegar a uma conclusão estatística dos percentuais de ataques.

Segue abaixo a explicação do objetivo da questão cinco, e as fórmulas utilizadas para chegar ao resultado final.

Na questão cinco teve como objetivo coletar informações sobre qual tipo de ataques essas empresas estavam mais sujeitas a receber, dentro de cinco categorias definidas.

O entrevistado tinha que colocar em percentual em cada categoria totalizando 100%. Segue abaixo um exemplo:

Ex: Rede Interna = 25% / Sistema Operacional =5% / Rede Externa 20%

/ Servidor de e-mail = 25% / Servidor de Internet (Servidor Web)= 25%

TOTAL = 100%

Após coletar as entrevistas foram colocadas as respostas na tabela abaixo:

Quadro 6 – Percentual de Ataques por categoria

Tabela para calcular Percentual de ataques:	**Ent1**	**Ent2**	**Ent3**	**Ent4**	**Ent5**	**Ent6**	**Ent7**	**Ent8**	**Ent9**	**Ent10**	**Total**	**Percentual Total**
Servidor de E-mail	25	15	50	25	35	40	30	25	30	10	285	28,50%
Servidor de Internet	25	30	30	25	20	10	20	25	30	5	220	22,00%
Rede Interna	15	30	5	25	20	30	20	25	20	30	220	22,00%
Rede Externa	20	15	10	20	15	10	20	15	10	15	150	15,00%
Sistema operacional	15	10	5	5	10	10	10	10	10	40	125	12,50%

Após colocar as informações de cada entrevistado na tabela, foi calculada uma regra de três em cada categoria, para se chegar a um percentual. Segue abaixo a explicação do cálculo:

Total = 285 + 220 + 220 150 + 125 = 1000

Servidor de E-mail = 1000 ----- 100 = 28,50%

285 ------ x

Servidor de Internet = 1000 ----- 100 = 22,00%

220 ------ x

Rede Interna= 1000 ----- 100 = 22,00%

220 ------ x

Rede Externa= 1000 ----- 100 = 15,00%

150 ------ x

Sistema Operacional= 1000 ----- 100 = 12,50%

125 ------ x

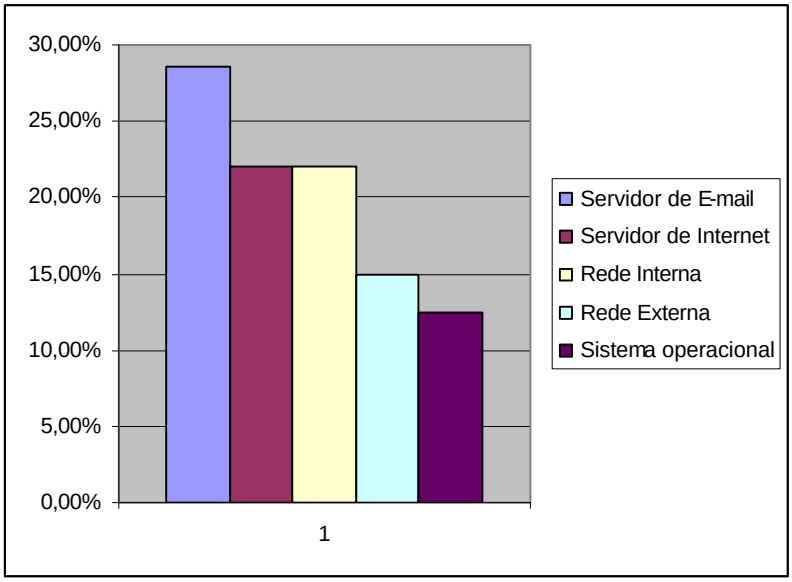

Ilustração 6–Gráfico com o percentual de Ataques por categoria

A sexta questão teve como objetivo identificar o grau de risco das categorias que foram definidas na questão anterior.

Na coleta de dados na questão seis foi desenvolvida uma questão, que tinha como objetivo relacionar em ordem crescente o grau de risco em cada categoria, com uma pontuação que poderia variar de 1 a 5. O maior risco foi definido como o de categoria 5.

Segue abaixo um exemplo:

Ex: Rede Interna = (2) / Sistema Operacional = (1) / Rede Externa (3)

/ Servidor de e-mail = (5) / Servidor de Internet (Servidor Web) = (4)

As informações coletadas foram inseridas na tabela abaixo:

Quadro 7 – Grau de Risco dividido por categoria

Tabela para calcular Grau de Risco	**Ent1**	**Ent2**	**Ent3**	**Ent4**	**Ent5**	**Ent6**	**Ent7**	**Ent8**	**Ent9**	**Ent**	**Total**	**Percentual**
Servidor de E-mail	4	3	4	5	5	5	5	5	5	5	46	30,67%
Rede Interna	5	2	5	4	4	4	3	4	1	4	36	24,00%
Servidor de Internet	3	4	3	3	3	3	4	2	4	3	32	21,33%
Rede Externa	2	5	2	1	2	1	2	1	3	1	20	13,33%
Sistema operacional	1	1	1	2	1	2	1	3	2	2	16	10,67%

Depois de colocar as informações de cada entrevistado na tabela, foi realizado um cálculo utilizando regra de três para chegar a um percentual final. Segue abaixo a explicação:

Total = 46 + 36 + 32 + 20 +16 = 150

Servidor de E-mail = 150 ----- 100 = 30,67%

46 ------ x

Servidor de Internet = 150 ----- 100 = 24,00%

36------ x

Rede Interna= 150 ----- 100 = 21,33%

32 ------ x

Rede Externa= 150 ----- 100 = 13,33%

20------ x

Sistema Operacional= 150 ----- 100 =10,67%

16 ------ x

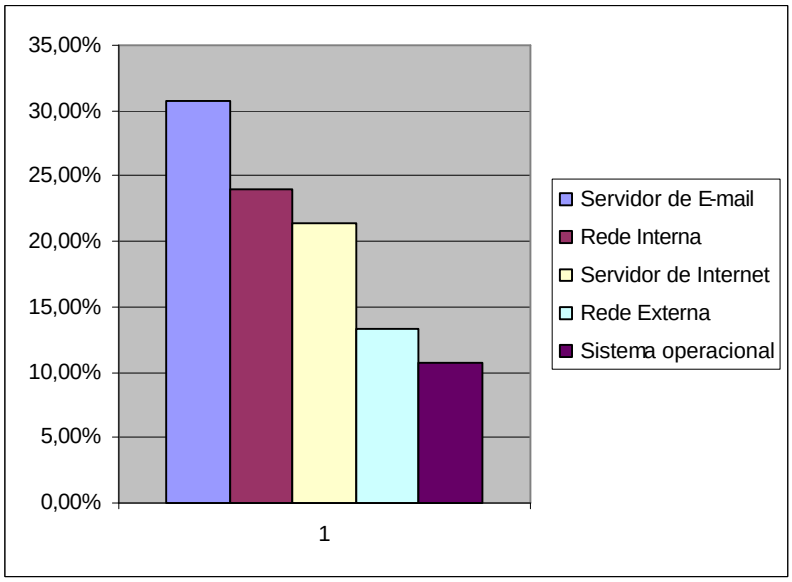

Ilustração 7-Gráfico com o grau de Risco por categoria

A sétima questão, a oitava, e a nona questão, foram desenvolvidas com o objetivo de serem questões abertas, para coletar informações mais flexíveis dos entrevistados.

Esse tipo de questão não é interessante para formar estatísticas, mas conseguem coletar informações importantes para um aprofundamento do assunto analisado.

As informações importantes relevantes à pesquisa, serão incluídas em uma recomendação de segurança que será descrita na conclusão do trabalho.

5 CONCLUSÃO

5.1 CONTRIBUIÇÕES

A pesquisa teve como objetivo ajudar Pequenas Empresas a estruturar soluções de segurança da Informação a baixo custo.

Cabe concluir que o Firewall que teve melhor pontuação foi á solução da Check Point safe@office 500 teve ótimas pontuações em todos os quesitos analisados, indicação, dificuldade de configuração, eficácia e abrangência. [18] [19]

O segundo colocado foi o Iptables, que conseguiu essa colocação, porque conseguiu um alto índice de indicações, e uma boa pontuação no parâmetro eficácia. Em compensação no parâmetro dificuldade de configuração e abrangência teve baixa pontuação. [5]

O terceiro colocado foi outra solução da Check Point o Firewall Utm -1 Edge que obteve menos indicações que o Iptables, mas em compensação obteve boas pontuações em todos os parâmetros analisados, inclusive dificuldade de configuração e abrangência [20].

O quarto colocado foi o Firewall Sonic Wall tz 190. Essa solução não obteve tantas indicações como as outras, mas conseguiu boas pontuações no parâmetro dificuldade de configuração e abrangência, no quesito eficácia sua pontuação foi abaixo dos outros analisados [16] [17] [21] [22].

Após essa etapa foram realizadas análise de custo e levantamento das descrições técnicas das soluções analisadas com as melhores pontuações.

Foram solicitados orçamentos para uma Empresa de Segurança para validar a Informações de custo de algumas soluções.

---

[5] Informações retiradas dos dados coletados

Conclui-se que nessa categoria às quatro soluções iriam atender a demanda de pequenas Empresas, mais algumas soluções com vantagens sobre as outras.

A solução da Check Point safe@office 500 para uma rede até 100 usuários, seria a solução mais recomendada para a maior parte das empresas, porque consegue excelentes pontuações em todos os parâmetros analisados. [6]

Essa solução utiliza várias tecnologias que são utilizadas pelos firewalls top de linha do mercado.

A solução foi desenvolvida com objetivo de atuar no mercado de Pequenas Empresas por isso os custos são muito baixos. Uma solução com appliance mais configuração e instalação está próximo de R$ 5.500[7]. [18] [19] [23]

O firewall que ficou em segundo lugar foi o Iptables, conclui-se que somente seria interessante utilizar essa solução se a Empresa tivesse o Hardware para ser utilizado no Firewall e não tivesse orçamento para a compra de novos equipamentos.

Com relação à terceira solução analisada Check Point o Firewall Utm -1 Edge foi uma solução que obteve bons resultados em todos os quesitos analisados, não tiveram tantas indicações mais os parâmetros analisados conseguiram ótimas pontuações.

A descrição técnica é muito parecida com a outra solução da Check Point safe@office 500 [20]. Essa solução tem uma vantagem, porque tem uma capacidade

---

[6] Informações analisadas após a pontuação dos softwares

[7] Essas informações foram retiradas de uma proposta comercial de uma Empresa de Segurança Brasileira.

para suportar maiores tráfegos do que as outras soluções analisadas podem suportar redes com mais de 100 usuários [20].

Com relação ao custo não é muito diferenciado, no Brasil a compra do Appliance com a configuração e instalação está em torno de R$ 7.000,00 [8]. Podendo variar de acordo com o fornecedor.

Conclui-se que para redes com mais de 100 usuários essa seria a melhor solução. [24]

O quarto colocado foi o Firewall Sonic Wall tz 190 essa solução não obteve tantas indicações como as outras, mas conseguiu boas pontuações no parâmetro dificuldade de configuração e abrangência, no quesito eficácia sua pontuação foi abaixo dos outras soluções analisadas.

Com relação à descrição técnica dessa solução é muito parecida com as características do Check Point safe@office 500 [16] [17], com algumas diferenças, por exemplo, a Sonic Wall utiliza uma tecnologia que se chama deep inspecion Packet em conjunto com a tecnologia UTM [21] [22], a Check Point utiliza State Inspecion Firewall utilizando UTM [20].

Nas características globais tem funcionalidades muito parecidas, inclusive os valores são praticamente Iguais, uma solução com appliance, configuração e instalação está em torno de R$ 5.500[9].

---

[8] Esse valor foi retirado de uma proposta comercial de uma de Segurança Brasileira.

[9] Esse valor foi retirado de uma proposta comercial de uma de Segurança Brasileira

A segunda categoria analisada foi à categoria Scanner de vulnerabilidade, nessa categoria ocorreu praticamente unanimidade entre os entrevistados, o Scanner de Vulnerabilidade Nessus, foi indicado por 90% dos entrevistados.

Após a coleta de dados e análise dos Resultados ficou constatada, que a maioria desses softwares é de fácil configuração e boa eficácia.

Entretanto a abrangência foi o parâmetro que deixou um pouco a desejar. Os três softwares que tiveram melhores pontuações foram o Nessus, Retina e o Core Impact [10].

Após análise de custo e descrição técnica desses produtos conclui-se que, realmente o software Nessus [25] seria a melhor solução.

A terceira categoria analisada foi dos Scanners de vulnerabilidade Web, essa categoria tem que ser realizado um estudo mais aprofundado com mais profissionais.

Na pesquisa não foi possível visualizar uma unanimidade entre os entrevistados, a minha percepção foi que essa categoria não é muito utilizada pelos profissionais que entrevistei.

A quarta categoria analisada foi á categoria IDS, que após a coleta dos dados e apresentação dos resultados demonstrou algumas características Interessantes.

Na opinião dos entrevistados foi praticamente unânime referente às dificuldades de configuração dos IDS, além desse detalhe a abrangência foi considerada baixa. Somente o IDS da Check Point IPS-1 [24] conseguiu boa

[10] Informações retiradas do quadro 5

pontuação nesse parâmetro. As soluções com melhores pontuações foram três Snort, Check Point IPS-1 [24], Source Fire [31].

O Snort foi o software que obteve a maior pontuação, com o maior número de indicações, baixa pontuação referente à dificuldade de configuração, e uma boa pontuação referente à eficácia. A pontuação da abrangência foi Razoável. O software não tem custo. [11]

O segundo colocado foi Check Point IPS-1, que não teve tantas indicações como o Snort, mais em compensação teve excelentes resultados em eficácia e abrangência.

O problema dessa solução foi o custo, quando foi realizada a análise de custo ficou inviável para uma Pequena Empresa [24].

O terceiro colocado foi o IDS Source Fire, que teve um resultado muito parecido com Snort mais com menos indicações.

Essa solução ocorreu o mesmo problema do IDS da Check Point, alto custo que foi um problema que ocorreu na maioria das soluções de IDS.

Após realizar o estudo ficou evidente a dificuldade de uma Pequena Empresa estruturar uma solução com IDS, porque uma solução que utilize o Snort é de difícil configuração, e as outras soluções analisadas foram de alto custo o que inviabiliza sua utilização.

Além das análises das soluções, foram realizados estudos estatísticos para gerar um percentual de ataques e riscos em cinco categorias definidas.

---

[11] Informações retiradas da coleta de dados

A coleta das informações do grau do risco foi muito produtiva porque demonstrou uma diferença, entre incidência de ataques e grau de risco.

O servidor de E-mail ficou em primeiro nos dois itens, mas o percentual de risco aumentou, outro detalhe importante foi o aumento do percentual de risco na rede Interna, passando para a segunda colocação. Isso demonstra como a rede interna tem um alto grau de risco alto nas corporações.

As últimas questões do questionário foram importantes, para coletar algumas recomendações de segurança para melhorar a infra-estrutura dessas empresas:

- Estruturar uma política de segurança na Empresa
- Estrutura uma campanha de conscientização dos usuários internos sobre as políticas a serem aplicadas e os seus benefícios e possíveis penas se não forem atendidas
- Estruturar uma política de atualizações com rotinas definidas
- O firewall da empresa tem que ser bem configurado, com uma solução confiável que utiliza a tecnologia UTM com deep inspection packet ou com a tecnologia Statefull Inspactions Firewall.
- Servidores de e-mail pela importância, têm que ser instalado um antivírus e um anti-spam atualizados.

Cabe concluir que, com todas as informações descritas na pesquisa, o objetivo da pesquisa foi alcançado, foram descritas soluções de baixo custo com bom nível de segurança.

5.2 LIMITAÇÕES DA PESQUISA

A grande limitação da pesquisa foi à dificuldade de realizar entrevistas para a coleta de dados, como o foco das entrevistas, eram profissionais que trabalham com segurança da Informação, existe uma grande resistência desses profissionais e das Empresas em fornecer informações.

Na maior parte das Empresas de Segurança existem regulamentos que somente permitem que algum funcionário, forneça algum tipo de entrevista se tiver autorização da Empresa o que acaba dificultando a coleta de dados.

Essa foi a maior limitação da pesquisa encontrar profissionais qualificados que realmente quisessem ajudar a pesquisa e autorização das Empresas de Segurança.

5.3 TRABALHOS FUTUROS

Poderiam ser desenvolvidos vários trabalhos futuros, um trabalho seria o de tentar mapear as diversas vulnerabilidades que pequenas empresas estão mais propícias a apresentar.

Como existe um grande universo de Pequenas Empresas, poderiam ser coletadas informações dentro dessas Empresas, realizando um trabalho com se estivesse sendo realizado uma análise de risco, para tentar realizar um mapeamento das vulnerabilidades que forem encontradas com maior incidência.

Outro trabalho poderia ser o de realizar um estudo mais aprofundado sobre a utilização dos softwares de análise de Vulnerabilidade Web.

REFERÊNCIAS

[1] KRUTZ, R.L.; VINES, D.V. **The Cissp Prep Guide Matering the Ten Domains of Computer Security**. New York: WILWE Computer Publishing, 2001.

[2] ASSUNÇÃO, M.F.A. **Segredos do Hacker Ético**. 2. ed. Florianópolis: Visual Books, 2008.

[3] FURMANKIEWIC, E; SANDRA. F. **Segurança Máxima**. 3. ed. Rio de Janeiro: Campus, 2001.

[4] CERT. **Denial of Service.** 2001**,** Disponível em: < http://www.cert.br/links/#denial_of_service>. Acesso em 07 de Julho. 2008.

[5] CERT. **Estatísticas**. 2008, Disponível em: <http://www.cert.br/stats/>. Acesso em: 07 de Julho. 2008.

[6] TANENBAUM, A.S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

[7] COMER, D.E. **Interligação em rede com TCP/IP Volume I Princípios, protocolos e arquitetura** Rio de Janeiro: Campus, 1995.

[8] WENSTROM, M.J. **Managing Cisco Network Security**. Indianapolis: Cisco Press, 2002.

[9] MODULO-EDUCATION-CENTER. **Security Officer modulo 2 parte 1.** Rio de Janeiro 2003.

[10] MODULO-EDUCATION-CENTER. **Security Officer modulo 2 parte 2.** Rio de Janeiro 2003.

[11] LOPES, R. **Firewalls**. 1997, Disponível em: <http://www.rnp.br/newsgen/9708/n3-1.html>. Acesso em 07 de Julho. 2008.

[12] CUFF, A. **Intrusion Detection Terminology (Part One)**.2006, Disponível em: <*http://www.securityfocus.com/infocus/1728*>. Acesso em: 07 de Julho. 2008.

[13] CUFF, A. **Intrusion Detection Terminology (Part Two)**.2006, Disponível em :< http://www.securityfocus.com/infocus/1733>. Acesso em 07 de Julho. 2008.

[14] COMPUTER-NETWORK-DEFENSE. **Network Intrusion Prevention Systems**.2007, Disponível em: <http://www.networkintrusion.co.uk/inline.htm>. Acesso em: 07 de Julho. 2008.

[15] SILVA, A.L.R. **Monografia Fácil – Ferramentas e exercícios Aplicáveis a Mestrado e Doutorado**. São Paulo: DVS, 2004.

[16] SONIC-WALL. **TzSeries Appliances**. 2008, Disponível Em: <http://www.sonicwall.com/lat/TZ_Series.html>. Acesso em 07 Julho.2008.

[17] SONIC-WALL. **Total Secure Solutions**. 2008, Disponível em: <http://www.sonicwall.com/lat/TotalSecure_Solutions.html>. Acesso em 07 de Julho. 2008.

[18] CHECK-POINT. **Safe@Office Appliances Proven Network Security for Small Businesses**. 2008, Disponível em: <http://www.checkpoint.com/products/safe@office/index.html>. Acesso em 07 de Julho. 2008.

[19] CHECK-POINT.**Check Point Introduces New Safe@Office Unified Threat Management Appliances with Integrated ADSL Modems**.2006, Disponível em: <http://www.checkpoint.com/press/2006/safe@adsl051606.html>. Acesso em 07 de Julho. 2008.

[20] CHECK-POINT. **Software Technologies Ltd. Descrição técnica Check Point UTM-1 EDGE**.2008, Disponível em :< http://www.checkpoint.com/products/appliances/index.html>. Acesso em 07 de Julho. 2008.

[21] SONIC-WALL. **Inspection Firewall Sonic Wall Deep Packet**.2008, Disponível em: <http://www.sonicwall.com/us/products/7543.html>. Acesso em 07 de julho. 2008.

[22] SONIC-WALL. **Unified Threat Management Perfomance.** 2008**,** Disponível em: <http://www.sonicwall.com/us/products/10025.html>. Acesso em 07 de Julho. 2008.

[23] CHECK-POINT. **Check Point Software Technologies Price List.** 2008, Disponível em: <https://pricelist.checkpoint.com/pricelist/US/PLUShomeOffice/holist.jsp.>. Acesso em: 07 de Julho. 2008.

[24] CHECK-POINT. **Check Point IPS -1**.2008, Disponível em :< https://pricelist.checkpoint.com/pricelist/US/PLUSGeneral/generallist.jsp#Power-1%20Security%20Appliances>. Acesso em 07 de Julho. 2008.

[25] TENABLE-NETWORK. **The Network Vulnerability Scanner**.2008, Disponível em: < http://www.nessus.org/nessus/>. Acesso em: 08 de Julho. 2008.

[26] EEYE. **Retina Network Security Scanner.** 2008, Disponível em: < http://www.eeye.com/html/products/retina/index.html>. Acesso em 08 de Julho. 2008.

[27] EEYE. **Purchase eEye Software.** 2008, Disponível em: < http://www.eeye.com/html/purchase/index.html>. Acesso em 08 de Julho. 2008.

[28] CORE-SECURITY. **Core Impact Overview**. 2008, Disponível em: < http://www.coresecurity.com/?module=ContentMod&action=item&id=32>. Acesso em 07 de Julho. 2008.

[29] CIRT. **Nikto Description**. 2008, Disponível em: <http://www.cirt.net/nikto2>. Acesso em 07 de Julho.

[30] ACUNETIX. **Acunetix Web Vulnerability Scanner Pricing**.2008, Disponível em: <http://www.acunetix.com/ordering/pricing.htm>. Acesso em: 07 de Julho. 2008.

[31] SOURCE-FIRE. **The Sourcefire 3D System**.2008, Disponível em: <http://www.sourcefire.com/products/3D/>. Acesso em 08 de Julho. 2008.