Parâmetros de Defesa Acessíveis a Empreendimentos de Pequeno e Médio Porte Utilizando *Pfsense*

Accessible Defense Parameters for Small and Medium-Sized Businesses Using *Pfsense*

Khawan M. Silva[1], Juliana S. Silva[1], Paulo B. Lopes[1]

[1]Departamento de Computação – Instituto Federal de Mato Grosso – Campus Cuiabá – Cel. Octayde Jorge da Silva – R. Profa Zulmira Canavarros, 95 – Centro, Cuiabá - MT, 78005-390 – Cuiabá-MT – Brasil.

khawan23@hotmail.com, {juliana.silva, paulo.lopes}@ifmt.edu.br

Abstract. *Throughout human history, the search for information has been one of the factors that made some countries and nations stronger and more advantageous than others. This has generated great concern for modern companies, since the invasion rates of their information systems have been increasing significantly. Thus, the aim of this research is to propose the implementation of Pfsense software as a firewall for greater control of a company's personal data and lower-cost accessibility. Therefore, the development of this research consisted of three phases: (i) literature review;(ii) analysis of the necessary requirements for the proposal; (iii) identification of the areas of application and mapping of future research for the development of the proposal. Based on the results, it was possible to present the elements necessary to create this mechanism and suggest places where this proposal could be implemented.*

Keywords: *cyber attack, corporate vulnerability, security strategy, and firewalls*

Resumo. *Com o decorrer da história da humanidade, a busca por informação foi um dos fatores que formou países e nações mais fortes e com vantagens sobre as outras – o que tem gerado grande preocupação das empresas modernas, uma vez que os índices de invasões de seus sistemas de informação vêm aumentando. Sendo assim, o objetivo deste trabalho é propor a implementação do software Pfsense como um firewall para um maior controle de dados pessoais de uma empresa, com o foco na acessibilidade de baixo custo. Deste modo, o desenvolvimento desta pesquisa compreendeu as seguintes fases: (i) revisão bibliográfica; (ii) análise dos requisitos necessários para a proposta; (iii) identificação das áreas de aplicação e mapeamento de futuras pesquisas para o desenvolvimento da proposta. Dentre os resultados encontrados, foi possível apresentar os elementos necessários para a criação desse mecanismo e sugerir locais onde poderá ser implementado.*

Palavras-chave: *ciberataque, vulnerabilidade empresarial, estratégia de segurança e firewalls.*

1. Introdução

Com o decorrer da história, o mundo passou por diversas guerras e conflitos. Quem ditava o rumo dos acontecimentos eram aqueles que tinham mais informações, obtidas por meio de ataques e roubos de dados. Logo, os países em busca de uma maior defesa desenvolveram o princípio de cibersegurança e alguns parâmetros de defesa – como filtragem de tráfego, gestão de vulnerabilidades, monitoramento de terceiros e uma autenticação mais forte.

Nesse sentido, o advento da tecnologia colaborou para a evolução e criação de *softwares* e *hardwares*, como *firewalls*, protocolos, controle de dados e equipamentos de defesa física, tornando as informações um pouco mais seguras. Ainda que com essa evolução, a cada ano que passa, os estudos mostram que invasões cibernéticas a empreendimento vêm aumentando. De acordo com a Comissão de Valores Mobiliários (CVM), em 2021 houve um crescimento de invasões cibernéticas de 220%, em comparação com o ano de 2020 (CNN, 2021).

À medida que empresas de âmbitos privados e públicos buscam sua evolução, por meio da tecnologia, acabam desencadeando um maior número de tentativas maléficas de acesso a dados pessoais (VIEIRA, 2021). A falta de recursos financeiros, muitas vezes, é um fator que impede que pequenas e médias empresas implementem medidas de segurança mais robustas, que requerem um investimento adicional. Diante deste cenário, o objetivo desse artigo é propor a implementação do *software Pfsense* como um *firewall* para um maior controle de dados pessoais de uma empresa, com o foco na acessibilidade de baixo custo.

Desta forma, este artigo está estruturado em 5 seções, incluindo esta introdução. A seção 2 apresenta os conceitos básicos sobre o tema. Em seguida, a seção 3 aborda a metodologia utilizada no desenvolvimento da pesquisa. Por fim, a seção 4, descreve a proposta de aplicação e, a seção 5, as considerações finais do trabalho.

2. Conceitos Básicos

Esta seção tem por objetivo abordar os conhecimentos específicos para um maior entendimento sobre os temas abordados nesta pesquisa.

2.1. Cibersegurança

O termo cibersegurança é usado para a proteção de dados de computadores (KASPERSKY, 2022) – que se tornou um dos principais requisitos de corporações e empreendimentos, uma vez que dados pessoais e confidenciais são alvos constantes de ataques (PEREIRA, 2021).

A cibersegurança vem para representar todos os métodos de proteção contra ameaças virtuais a dados e informações; alguns exemplos mais comuns dessas ameaças são ataques cibernéticos, *Spywares*, *Adwares* e *Ransomwares* (KASPERSKY, 2022).

De acordo com os dados do relatório da *Riskbased* (RISKBASED, 2020), de janeiro a setembro de 2019, 7,9 bilhões de registros foram comprometidos por violações de dados. Diante deste cenário surge uma preocupação: como dispor de recursos de *hardware* e *software* para o monitoramento de uma rede? Detalhes adicionais são descritos a seguir.

2.2. *Hardware* e *Software* de Monitoramento de Rede

Com o avanço das Tecnologias de Informação e Comunicação, a demanda por segurança de dados aumentou significativamente, impulsionando o desenvolvimento de dispositivos especializados. Esses dispositivos combinam hardware e software para

fornecer controle e proteção de dados. No entanto, devido aos custos elevados dos componentes, esses dispositivos tornaram-se acessíveis apenas para algumas empresas e indivíduos privilegiados. (JANONE, 2021).

No mercado atual, diversas empresas e projetos concentram seus esforços na integração de hardware e software para monitoramento de rede. Os principais desenvolvimentos se concentram no gerenciamento, monitoramento e análise não apenas da rede, mas também dos dispositivos conectados a ela. No entanto, essas soluções costumam ter preços que variam de US$ 300,00 a US$ 1.995,00, tornando-as inacessíveis para muitas empresas de pequeno e médio porte (Duarte, 2020). Diante desse cenário, há uma demanda crescente por opções de baixo custo, como a que será apresentada a seguir.

2.3. *Software* de Monitoramento *Pfsense*

O *Pfsense* é um *software* de monitoramento *open source*, criado em 2004, por Buechler e Scott Ullrich (TECHLISE, 2020), que foi projetado para operar em *hardware* convencional de mercado ou máquinas virtuais. Sua arquitetura é altamente flexível e modular, possibilitando que os administradores personalizem sua configuração conforme as exigências da rede, por meio de uma interface *web* intuitiva. Isso torna a administração e o gerenciamento do *Pfsense* mais simples.

O *Pfsense* pode ser controlado por um campo de interação *web*, facilitando o controle e o monitoramento dos dados que serão trabalhados (NEVES, 2014), de forma acessível e gratuita, necessitando apenas de um *hardware* de baixo custo. Assim, sua configuração envolve a definição de interfaces de rede, configuração de regras de *firewall*, configurações de *Virtual Private Network (VPN)*, definição de *Virtual Local Area Network* (VLANs) e outras políticas de segurança. A flexibilidade do *Pfsense* permite que ele seja adaptado para atender a uma ampla variedade de cenários de rede.

Uma vez que se tenha realizado uma breve descrição do referencial teórico deste artigo, a seção seguinte apresenta o material e os métodos utilizados neste estudo.

3. Material e Métodos

O desenvolvimento desta pesquisa compreendeu as seguintes fases: (i) revisão bibliográfica; (ii) análise dos requisitos necessários para a proposta; (iii) identificação das áreas de aplicação para o desenvolvimento da proposta.

Na etapa (i), foram utilizadas como apoio as ferramentas de busca *Google Acadêmico* e a Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), com o uso das seguintes palavras-chave: “segurança de dados”, “implementação *Pfsense*”, “cibersegurança” e “gerenciamento de rede”. A partir de então, foram mapeados artigos publicados entre os anos de 2001 e 2021.

Em seguida, na etapa (ii) foram definidos os recursos de *hardware* e de *software* necessários para o desenvolvimento do projeto – os quais estão descritos na seção a seguir (4. Proposta de Aplicação). Por fim, na etapa (iii) foram mapeadas algumas áreas de possível implementação do projeto.

4. Proposta de Aplicação

A ideia deste artigo é propor um método de controle de dados e aumento de segurança para empresas que não podem arcar com licenças caras de *software* e *hardwares* de alto custo. Para isso, propõe-se construir um servidor com peças usadas, incluindo um pente de memória *RAM DDR3* de *2GB*, uma placa de rede *PCI-E TP-link TG-3468*, uma placa mãe *LGA 1155 H61 DDR-3*, um *hub* de *internet* e, por fim, um processador *I5-3470*.

Tais configurações são suficientes para o funcionamento da proposta, devido ao baixo nível de processamento necessário para o *Pfsense*. Ressalta-se que o foco são estabelecimentos de pequeno e médio porte, que tenham de 1 a 10 computadores a serem controlados e monitorados. Já para o controle e o acionamento do *firewall*, a proposta é que sejam utilizados o *software Pfsense* e o sistema operacional *Berkeley Software Distribution* (*FreeBSD*).

Implementar um método de controle de dados fortalece a segurança da empresa contra ataques maliciosos e indiscrições internas, protegendo suas informações confidenciais. Além disso, otimiza a eficiência da rede ao prevenir sobrecargas no servidor e melhorar a velocidade de transmissão de dados. Dessa forma, a empresa reduz o risco de perda de informações cruciais.

Após o primeiro acesso à interface *web*, o usuário configurará as permissões de acesso a qualquer *site*, aplicativo e à própria rede. Utilizando o DHCP (*Dynamic Host Configuration Protocol* – Protocolo de Configuração Dinâmica de Endereços de Rede), será possível gerar e configurar um IP (*Internet Protocol* – Protocolo de Internet) para cada máquina, podendo, assim, configurar parâmetros individuais ou para uma determinada faixa de IPs.

Ademais, será possível bloquear *sites* e aplicativos maléficos, aumentando, assim, o grau de segurança e controle dos dados transmitidos nessa rede local. De maneira mais técnica, a *internet*, vinda externamente, é passada por uma conexão WAN (*Wide Area Network* – Rede de Longa Distância) diretamente para o servidor, onde sofrerá todas as restrições estabelecidas pelo usuário, devido ao *firewall Pfsense*. Em seguida, a *internet* é direcionada ao *hub* para a distribuição dos dados, por meio de uma conexão LAN (*Local Area Network* – Rede Local), para todos os computadores locais ou, alternativamente, para uma Zona Desmilitarizada (DMZ), que é parte de uma rede de computadores configurada para fornecer uma camada adicional de segurança. Essa separação protege a rede interna (geralmente a rede corporativa) da rede externa (geralmente a Internet) ou de outras redes não confiáveis, como mostrado na Figura 1.

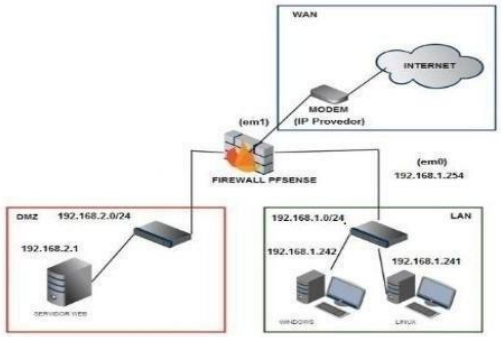

Figura 1. Topologia da Rede (adaptado de NEVES et al., 2014)

Uma vez conectado em toda essa rede, o usuário, com o controle do servidor, pode observar os dados passados pelos computadores da rede e controlar o tráfego de informações, além de ter acesso remoto, utilizando uma VPN.

Assim, o *Pfsense* emerge como uma ferramenta multifuncional que atende a uma ampla gama de necessidades, por meio da qual é possível construir infraestruturas de segurança sólidas, proteger os dados, aprimorar a eficiência operacional. Essa versatilidade é crucial para o sucesso contínuo das organizações em um ambiente de negócios cada vez mais orientado por dados.

5. Considerações Finais

Este artigo teve como objetivo propor medidas de segurança acessíveis a empresas que

não possuem condições financeiras para adquirir *firewalls* pagos e *hardwares* caros, utilizando o *software* de monitoramento *Pfsense* como base para o projeto – com foco na eficiência, praticidade, qualidade e acessibilidade. Durante a pesquisa inicial sobre o tema, foi observado que existem muitas possibilidades e locais de implementação, mostrando que, mesmo com diversos trabalhos já realizados, ainda é possível explorar e agregar mais ao tema, como por meio desta proposta.

A recomendação é que esta proposta seja aplicada em empresas de pequeno e médio porte, como na área de salões, clínicas médicas e odontológicas, farmácias, pizzarias e restaurantes - todos aqueles empreendimentos que possuem acesso à *internet* e circulam dados pessoais de clientes da empresa.

Como possíveis projetos futuros, tem-se a ideia de desenvolver um *software* personalizado de *backup* em nuvem que atenda às necessidades específicas das pequenas e médias empresas. Isso permitiria que essas empresas armazenassem seus dados de forma segura na nuvem, garantindo a recuperação rápida, em caso de perda de dados. Além de desenvolver uma solução que permita às empresas separar o acesso às informações por departamento ou equipe. Isso agregaria maior controle e eficiência, pois cada departamento teria acesso apenas às informações relevantes, aumentando a segurança e facilitando a gestão de dados.

Referências

CNN. **Ataques cibernéticos a empresas brasileiras crescem 220% no 1º semestre de 2021.** 2021. Disponível em: https://www.cnnbrasil.com.br/economia/ataques-ciberneticos-aempresas-brasileiras- crescem-220-no-1-semestre-de-2021. Acesso em: 7 set. 2023.

DUARTE, L. **10 Melhores Ferramentas de Monitoramento de Rede**. 2019. Disponível em: https://comoaprenderwindows.com.br/utilitarios/10-melhores-ferramentas-de-monito ramento-de-rede/. Acesso em: 7 set 2023.

JANONE, L. **Ataques cibernéticos a empresas brasileiras.** 2021. Disponível em: https://www.cnnbrasil.com.br/economia/ataques-ciberneticos-a-empresas-brasileirascre scem-220-no-1-semestre-de-2021/. Acesso em: 7 set. 2023.

KASPERSKY. **O que é Cibersegurança.** 2022. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. Acesso em: 10 out. 2022.

NEVES, F. C. et al. **Implantação de Firewall Pfsense.** 2014. 67f. Trabalho de Conclusão de Curso (Graduação em Sistema de Telecomunicação) - Universidade Tecnológica Federal do Paraná, Curitiba.

RISKBASED. **Cybersecurity-statistics.** 2020. Disponível em: https://flashpoint.io. Acesso em: 6 set. 2023.

TECHLISE. **Pfsense:** tudo que você precisa saber. 2020. Disponível em: https://www.techlise.com.br/blog/pfsense-tudo-que-voce-precisa-saber. Acesso em: 6 set. 2023.

VIEIRA, J. R. **Lei geral de proteção de dados: benefícios e obstáculos diante da atividade empresarial.** 2021. 42 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade de Direito de Vitória, Vitória.