SEGURANÇA EM REDES DE COMPUTADORES

Juliano Aparecido Martins
Faculdade Tecnologica de Assis
juliano.martins@fatec.sp.gov.br

Fabio Eder Cardoso
Faculdade Tecnologica de Assis
fabio.cardoso6@fatec.sp.gov.br

RESUMO

Este estudo investiga a importância crescente da segurança em redes de computadores na sociedade contemporânea. Destacando a evolução dos sistemas computacionais de uma abordagem centralizada para distribuída, enfoca os desafios de segurança resultantes dessa mudança. A pesquisa busca fornecer informações que auxiliem corporações na mitigação de ameaças cibernéticas e no aprimoramento das estratégias de segurança existentes. Baseada em revisão bibliográfica, a metodologia consolida teorias e conceitos-chave de autores renomados. Profissionais de segurança desempenham um papel vital na identificação, análise e resposta a vulnerabilidades e ameaças. Soluções como firewalls e sistemas de detecção/prevenção de intrusões são cruciais na proteção contra ataques cibernéticos. A complexidade do cenário de segurança atual é ressaltada pela variedade de ameaças, demandando investimentos críticos em segurança de redes e a aplicação de princípios fundamentais para preservar a segurança da informação.

Palavras-chave: Segurança; Redes; Ameaças; Profissionais.

ABSTRACT

This study investigates the increasing importance of network security in contemporary society. Highlighting the evolution of computer systems from a centralized to a distributed approach, it focuses on the security challenges arising from this shift. The research aims to provide insights to assist corporations in mitigating cyber threats and enhancing existing security strategies. Based on a literature review, the methodology consolidates theories and key concepts from renowned authors. Security professionals play a vital role in identifying, analyzing, and responding to vulnerabilities and threats. Solutions such as firewalls and intrusion detection/prevention systems are crucial in safeguarding against cyber-attacks. The complexity of the current security landscape is underscored by the variety of threats, necessitating critical investments in network security and the application of fundamental principles to preserve information security.

Keywords: Security; Networks; Threats; Professionals.

1 INTRODUÇÃO

Na atualidade, praticamente se torna inconcebível para a sociedade manter-se de forma adequada sem o indispensável suporte das redes de computadores. À medida que o tempo avança, um número crescente de pessoas adquire dispositivos com a capacidade de se conectar à Internet, permitindo-lhes acessar uma ampla gama de serviços oferecidos através dessa rede, como o envio de *e-mail*, redes sociais e o uso de serviços de mensagens instantâneas (MACEDO *et al.,* 2018)

Macedo (2018) complementa que com o avanço da tecnologia e o crescente número de pessoas adquirindo dispositivos com capacidade de conexão à Internet, as redes de computadores mudaram fundamentalmente a estrutura dos sistemas computacionais. Inicialmente, os sistemas eram organizados em torno de um único computador que realizava todas as tarefas de processamento e armazenamento, devido ao alto custo de aquisição de múltiplas máquinas. No entanto, à medida que os computadores se tornaram mais poderosos, compactos e acessíveis, tornou-se viável para empresas e indivíduos adquiri-los, levando a uma transição de sistemas centralizados para uma abordagem distribuída, com vários computadores interconectados (MITSHASI, 2011).

Essa mudança na estrutura dos sistemas computacionais trouxe consigo desafios adicionais, especialmente relacionados à segurança. De acordo com Mitshasi (2011), com o aumento da utilização de componentes de redes e da Internet, ocorreu um grande crescimento no número de invasões e infecções por vírus, destacando a necessidade crítica de investimento na área de segurança de redes.

O objetivo deste trabalho é conduzir uma pesquisa bibliográfica em artigos, livros e em sites especializados, visando compreender e sintetizar o estado atual do conhecimento acerca da segurança de sistemas de informação corporativos e das estratégias de proteção contra software mal-intencionados. Essa investigação tem por propósito identificar as principais ameaças cibernéticas enfrentadas pelas corporações e realizar uma análise crítica das estratégias de segurança em vigor, abrangendo elementos como criptografia, assinatura digital, certificado digital, autenticação e protocolos, com o intuito de avaliar suas eficácias e limitações.

Adicionalmente, busca-se mapear as melhores práticas e tendências emergentes na área de segurança de sistemas de informação corporativos, fundamentando-se na literatura disponível. O escopo final é fornecer uma base de informações abrangente que não apenas contribua para a compreensão das ameaças cibernéticas enfrentadas pelas corporações, mas também promova o aprimoramento contínuo das estratégias de segurança existentes.

A justificativa deste trabalho se apoia na grande importância das corporações em manter a segurança de seus sistemas de informação. O estudo é relevante devido à compreensão de

que as empresas modernas dependem cada vez mais desses sistemas para garantir a confiabilidade, integridade e disponibilidade de suas operações. No entanto, enfrentam desafios significativos devido à falta de informações detalhadas sobre ameaças cibernéticas e estratégias de segurança eficazes. Essa carência de informações cria um ambiente propício a vulnerabilidades e ataques, com potenciais impactos graves (ALVES, 2021).

Portanto, este estudo acadêmico é de grande importância para o autor, proporcionando a oportunidade de adquirir novos conhecimentos e aprofundar os tópicos previamente estudados na instituição. Adicionalmente, desempenha um papel fundamental ao transmitir eficazmente o conteúdo, potencialmente inspirando tanto organizações quanto futuros alunos do curso de Gestão da Tecnologia da Informação.

2 DESENVOLVIMENTO

2.1 Segurança de redes de computadores

No período em que as informações eram exclusivamente armazenadas em formato físico, a segurança se caracterizava por uma relativa simplicidade. Bastava a precaução de trancar documentos em locais específicos e restringir o acesso físico a esses espaços. Com a evolução tecnológica e a introdução de computadores de grande porte, a estrutura de segurança passou por certo aprimoramento, incorporando controles lógicos, embora ainda centralizados (TCU, 2012). No entanto, hoje em dia, sistemas de computadores enfrentam diversas ameaças à segurança, como códigos maliciosos, spams, ataques de negação de serviço, riscos à privacidade, fraudes e anomalias de rede. Essas ameaças estão evoluindo para níveis cada vez mais sofisticados (KAWAKANI, 2014).

O aumento das atividades maliciosas é, em grande parte, atribuível à ineficácia das soluções existentes na identificação, redução e interrupção desse tipo de tráfego. Normalmente, a eficácia das soluções atuais é comprometida devido às altas taxas de falsos alarmes e à falta de integração com outras soluções ou até mesmo com a infraestrutura de rede. Além disso, muitas dessas soluções requerem intervenção humana, como configuração, adaptação e ajustes, para funcionar adequadamente (HENKE *et al.,* 2011).

Stallings (2015) destaca que a área de segurança de redes abrange abordagens para desviar, prevenir, detectar e resolver incidentes de segurança relacionados à transferência de informações. Na busca por soluções mais eficazes e precisas, especialmente aquelas voltadas para o tráfego malicioso na Internet, muitos pesquisadores e empresas de segurança têm dedicado tempo e recursos para transformar a aprendizagem de máquina em uma ferramenta poderosa e eficaz na proteção de redes de computadores (HENKE *et al*., 2011).

A segurança de redes é essencial para proteger informações e sistemas contra ameaças cibernéticas. Os profissionais desse campo devem manter-se atualizados com as tendências em segurança, possuir habilidades técnicas avançadas e adotar uma abordagem proativa para antecipar e mitigar os riscos de segurança. Dessa forma, eles contribuem para preservar a integridade, confidencialidade e disponibilidade dos recursos de TI corporativos, garantindo a continuidade dos negócios e a proteção dos ativos da organização (SANTOS, 2023).

Tanto na Ciência da Informação quanto na Tecnologia da Informação, a segurança da informação repousa sobre princípios fundamentais, tais como confidencialidade, integridade, disponibilidade, autenticidade, dentre outros, conforme descritos na literatura relevante (ANDRADE, 2018). A violação de qualquer um desses princípios tem um impacto negativo na organização. Não há consenso na literatura sobre a superioridade de um princípio em relação ao outro em termos de importância, já que todos desempenham um papel crucial na busca pela segurança (MACHADO, 2014).

A segurança de redes de computação não deve ser abordada unicamente como uma preocupação técnica, mas sim como uma questão de governança corporativa. É crucial que a alta administração da empresa esteja plenamente envolvida no processo decisório relacionado à segurança de rede, estabelecendo, assim, uma cultura organizacional que valorize a segurança da informação (SANTOS, 2023).

2.2 Protocolo de Segurança

Um protocolo é fundamentalmente um conjunto de regras e convenções que permitem a comunicação entre computadores, como se fossem sistemas que falam a mesma “língua". É uma estrutura que define como a informação deve ser transmitida, recebida e interpretada, proporcionando um meio para a interação eficaz entre dispositivos. Um dos protocolos mais amplamente utilizados em redes é o TCP/IP, que representa "Protocolo de Controle de Transmissão/Protocolo Internet" (ALVEZ, 2021).

Alvez (2021) reforça que o TCP/IP é responsável por permitir que computadores enviem e recebam informações solicitadas pelos usuários. Ele é a espinha dorsal da comunicação na Internet e em muitas redes, assegurando uma transferência de dados confiável e eficiente entre dispositivos interconectados. Assim, os protocolos desempenham um papel essencial na garantia de que os sistemas possam comunicar-se de maneira eficaz e compreensível.

2.3 Ameaças à segurança

As ameaças e os perigos sempre acompanharão todas as atividades humanas (RIBEIRO, 2012). Nesse contexto, torna-se logicamente inviável evitar por completo danos e perdas digitais,

sendo mais realista a abordagem de minimizar ao máximo a cadeia de riscos (ANDRADE, 2018). Inúmeros problemas nas redes decorrem de ameaças de intrusos operacionais. Contudo, diversas organizações minimizam esses novos vírus, seja por falta de familiaridade com o assunto ou pela percepção de que o investimento necessário carece de justificativa (ALVES, 2021).

A evolução das ameaças cria novos obstáculos para a segurança dos computadores, seguindo um ciclo contínuo. Esse ciclo começa com a detecção de novas ameaças, que posteriormente são analisadas e, por fim, são implementadas medidas de prevenção. No entanto, este ciclo é desequilibrado, uma vez que somente uma fração das novas ameaças é identificada e apenas uma parcela das ameaças identificadas recebe tratamento em tempo hábil (KAWAKANI, 2014).

Segundo Andrade (2018), devido ao aumento constante das ameaças cibernéticas, a segurança no ambiente empresarial é uma preocupação cada vez mais urgente, pois essas ameaças, como *malware, phishing*, ataques de negação de serviço e *ransomware*, podem causar sérios danos às empresas. Com a evolução da tecnologia, a segurança da rede corporativa se tornou essencial para preservar a integridade dos dados e a continuidade dos negócios.

2.3 Tipos de Ameaças

Para abordar as ameaças em sistemas computacionais, é essencial explorar detalhadamente os diversos tipos de riscos existentes, compreendendo suas características, os métodos de ataque que empregam e os comportamentos que manifestam quando infiltrados em um sistema (ALVES, 2021).

2.3.1 Vírus

Um vírus ou código malicioso é um tipo de *malware* que depende de um hospedeiro para executar suas funções, que consistem em modificar o funcionamento normal de um computador, muitas vezes sem o conhecimento do usuário (MACHADO, 2014). Portanto, um vírus só pode se propagar e causar danos em um sistema computacional quando é executado pelo usuário, caso contrário, ele não se replicará nem causará prejuízos (ALVES, 2021).

2.3.2 Malware

Malware é uma categoria de ameaças desenvolvida com diversos objetivos, incluindo ganho financeiro, roubo de dados confidenciais, autopromoção e vandalismo, uma vez que esses

programas têm a capacidade de executar comandos e acessar informações nos computadores infectados (KAWAKANI, 2014).

Kawakani (2014) ainda explica que, a infecção de um usuário pode ocorrer de diversas maneiras. Fora de uma rede de computadores, um usuário pode ser vítima por meio de pen drives infectados, programas autoexecutáveis, ou ao abrir arquivos que contenham o código malicioso. No ambiente *online*, os *malwares* podem ser encontrados em páginas da *web* maliciosas (muitas vezes acessadas através de *links* falsos), em *e-mails* e em arquivos disponíveis para *download*. Além disso, os usuários também podem ser infectados por meio de invasões que resultam na instalação direta de arquivos mal-intencionados.

2.3.3 Spyware

O *spyware* é um programa desenvolvido com o propósito de monitorar e coletar informações e atividades realizadas em um sistema. Sua classificação como legítimo ou malicioso depende da maneira como é instalado, do tipo de informação monitorada e do uso subsequente dessas informações. Ele pode ser obtido por meio de *downloads, e-mails,* mensagens instantâneas, conexões diretas com compartilhamento de arquivos e até mesmo em contratos de licença para o uso de um *software*. Embora não seja necessariamente malicioso, seu uso pode variar amplamente, desde monitorar a atividade do sistema por terceiros até ações mais prejudiciais (KAWAKANI, 2014).

2.3.4 Spam

O problema do *e-mail* não solicitado, conhecido como spam, é uma questão amplamente reconhecida pelos usuários da Internet. O *spam* resulta na perda de tempo dos usuários e na sobrecarga dos recursos computacionais. Além disso, os spams desempenham um papel na disseminação de ameaças como Cavalos de Troia, *vírus, worms e spywares*, além de serem usados para realizar ataques de *phishing* e promover vendas ilegais de produtos. O *spam* é especialmente problemático devido ao seu baixo custo e à capacidade de atingir uma ampla escala (ANDRADE, 2018).

2.3.5 Vulnerabilidade

Conforme Machado (2014) destaca, as vulnerabilidades são falhas que, por si só, não provocam incidentes, pois são elementos passivos que demandam a ação de um agente causador ou favorável para serem exploradas. O que torna essas vulnerabilidades preocupantes é a dependência de um agente causador, como um hacker, malware ou mesmo uma falha

acidental por parte de um usuário, para serem efetivamente exploradas, transformando-se, assim, em ameaças à segurança.

2.3.6 Bots

Um bot é um programa que, ao explorar vulnerabilidades, permite que um invasor assuma o controle remoto do computador da vítima. Essa operação ocorre sem o conhecimento da vítima, permitindo que o invasor realize ações maliciosas diretamente do computador controlado, frequentemente chamado de "computador zumbi". Utilizando esse "computador zumbi," é possível atacar outras vítimas, roubar dados e enviar spam. Essa habilidade de controle remoto torna os bots uma ferramenta perigosa e versátil nas mãos de indivíduos mal-intencionados (KAWAKANI, 2014).

2.4 Soluções Existentes

De acordo com Andrade (2018), a Internet se destaca como uma das poucas plataformas operacionais descentralizadas, o que pode ser tanto uma vantagem quanto uma vulnerabilidade, contribuindo para o aumento do tráfego malicioso. Diversas soluções têm sido desenvolvidas para enfrentar esse desafio ao longo dos anos, porém, as atuais soluções de segurança enfrentam limitações na identificação e interrupção do tráfego indesejado, além de exigirem intervenção humana para funcionar corretamente, evidenciando a necessidade de melhorar a eficácia e automatização da segurança cibernética (ANDRADE, 2018).

Alves (2021) argumenta que, na área da segurança, é imperativo resolver problemas rapidamente para evitar que se tornem mais complexos e representem riscos inaceitáveis de exposição de informações confidenciais a criminosos. Portanto, investir em soluções mais eficazes e precisas, como a aprendizagem de máquina, tem sido uma prioridade para pesquisadores e a indústria de segurança de software, representando uma evolução promissora na defesa cibernética (ANDRADE, 2018).

Profissionais de segurança desempenham um papel crucial na proteção de redes de computadores, identificando vulnerabilidades, desenvolvendo políticas de segurança, implementando soluções de proteção e monitorando constantemente a rede em busca de atividades suspeitas (OLIVEIRA e MALAGOLLI, 2016). Eles também são responsáveis pela gestão de firewalls e pela promoção de uma cultura de segurança nas empresas, treinando colaboradores e conscientizando sobre boas práticas (MCCLURE *et al*., 2014). Em suma, os profissionais de segurança desempenham um papel vital na proteção contra ameaças

cibernéticas, sendo essencial manter-se atualizado com as tendências em segurança e adotar uma abordagem proativa para antecipar e mitigar riscos (SANTOS, 2023).

3 METODOLOGIA

O avanço tecnológico trouxe sistemas distribuídos e desafios em segurança, este estudo acadêmico enfoca a importância da segurança em redes de computadores. Para descrever a metodologia empregada na busca dos objetivos deste trabalho, é crucial compreender que o método "...é a ordem que se deve impor aos diferentes processos necessários para atingir um certo fim ou um resultado desejado. Nas ciências, entende-se por método o conjunto de processos empregados na investigação e na demonstração da verdade" (CERVO E BERVIAN, 2002, p. 23).

A revisão da literatura desempenhou um papel crucial na sustentação do conteúdo, retiradas de materiais previamente publicados, como livros, artigos e recursos da internet, entre outros (ALMEIDA, 2017). Com o intuito de compreender as teorias e conceitos-chave relevantes para a pesquisa, as fontes utilizadas para esta revisão incluem artigos acadêmicos obtidos no SCIELO e no Google Acadêmico, de autores como Alves (2021), Mitshasi (2011), Macedo (2018), entre outros.

Assim, a presente pesquisa se consolida sobre uma base sólida, incorporando uma metodologia que valoriza a revisão bibliográfica como instrumento essencial para a construção do conhecimento. A análise crítica e a síntese de trabalhos existentes proporcionam uma compreensão profunda e embasada sobre a segurança em redes de computadores, consolidando assim a relevância deste estudo no contexto atual.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

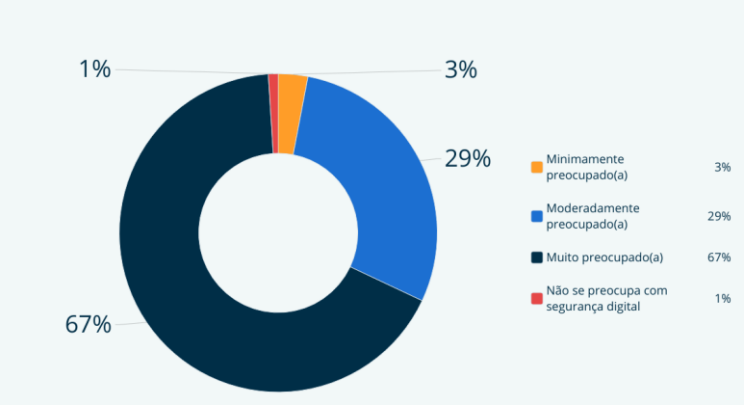
A abordagem da segurança em redes de computadores é marcada pela sua complexidade, representando um desafio para as organizações que buscam lucratividade, eficiência de tempo e redução de custos. Nesse contexto, a segurança torna-se uma ferramenta fundamental, exigindo que os procedimentos e recursos dedicados a ela sejam priorizados e constantemente avaliados no ambiente corporativo (COSTA *et al.,* 2012).

Segundo Henke *et al.* (2011), embora a maioria dos usuários de redes sociais não represente uma ameaça, indivíduos mal-intencionados são atraídos para essas plataformas devido à sua acessibilidade e à abundância de informações pessoais disponíveis, que podem ser exploradas para realizar ataques de engenharia social e disseminação de códigos maliciosos. Com o aumento dos computadores pessoais e das redes interconectadas globalmente, os

aspectos relacionados à segurança alcançaram um nível significativo de complexidade, demandando o contínuo desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação tornaram-se essenciais para a sobrevivência das instituições modernas.

Um levantamento conduzido por Gava em 2022, que colheu a opinião de 714 brasileiros de todas as regiões do país entre os dias 16 e 23 de junho de 2021, desempenhou um papel importante na ampliação da compreensão sobre a segurança digital. Segundo o estudo, demonstrou-se que 6 em cada 10 brasileiros consideram-se muito preocupados com a segurança digital.

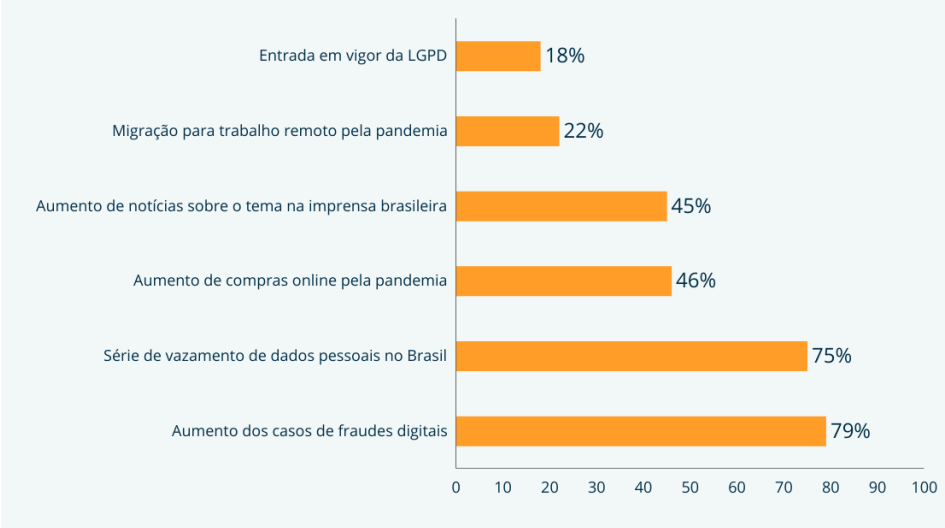
Figura 1 – Nível de preocupação com segurança digital.



Fonte: GAVA, Marcela. Segurança Digital, 2012

Conforme destacado por Gava (2022), os casos de vazamento de dados pessoais estão se tornando mais frequentes no Brasil, conforme revelado por um estudo do MIT. O referido estudo aponta um expressivo aumento de 493% nesse tipo de incidente. Adicionalmente, as tentativas de fraude digital também estão em ascensão, evidenciando um aumento de 53% entre 2020 e 2021 nesse tipo de crime.

Figura 1 – Motivos que preocupam as pessoas com segurança digital.



Fonte: GAVA, Marcela. Segurança Digital, 2012

A detecção de agentes automatizados, como worms e vírus, pode ser realizada por meio da análise avançada de padrões de tráfego na rede de saída. Esses agentes maliciosos deixam rastros distintos em termos de comportamento de comunicação, padrões de transferência de dados e características específicas de interação com sistemas remotos. Ao examinar padrões de tráfego de saída, é possível identificar anomalias indicativas da presença desses agentes automatizados, incluindo comunicações suspeitas, transferências não autorizadas ou atividades não alinhadas com o comportamento típico de usuários legítimos (HENKE *et al.,* 2011).

Menezes et al. (2015) enfatizam a necessidade de um conhecimento abrangente sobre os protocolos de rede para realizar testes de segurança. Essa compreensão vai além do uso dos protocolos, incluindo a aplicação habilidosa desses protocolos nas ferramentas específicas utilizadas durante os testes. Os protocolos de rede, especialmente a TCP/IP, representam a linguagem pela qual os computadores se comunicam, sendo essencial compreender detalhadamente esses protocolos para lidar eficientemente com as informações transmitidas entre computadores.

A eficácia e conformidade dos firewalls são essenciais, conforme ressaltado por Costa *et al.* (2012), destacando seu papel na filtragem de conteúdo e no cumprimento das políticas de uso da Internet. A gestão do risco em segurança da informação, discutida por Henke *et al.* (2011), é crucial para manter a integridade e reputação da instituição diante das ameaças, invasões e vazamentos de informações. Menezes (2015) destaca que a implementação de medidas de segurança demanda um cuidadoso trabalho a longo prazo, sendo que o modelo de proteção apresentado neste estudo oferece uma excelente relação custo/benefício, contribuindo para a maximização de lucros e a minimização do tempo investido.

O estudo recomenda-se para todos interessados no tema que buscam uma posição sólida no mercado atual. A análise detalhada desses padrões envolve o uso de ferramentas avançadas de monitoramento de rede, sistemas de prevenção de intrusões e algoritmos de detecção de ameaças, sendo crucial para distinguir entre tráfego legítimo e atividades potencialmente maliciosas e proporcionar uma resposta eficaz para proteger a integridade e segurança da rede (MACHADO, 2014).

5 CONSIDERAÇÕES FINAIS

Diante do crescente papel das redes de computadores na sociedade contemporânea, este estudo destaca a grande importância da segurança nesse contexto dinâmico e desafiador. A evolução tecnológica transformou fundamentalmente a estrutura dos sistemas computacionais, passando de uma abordagem centralizada para sistemas distribuídos interconectados. No entanto, essa transição trouxe consigo desafios substanciais, especialmente em relação à segurança.

Este estudo destaca a importância da segurança em redes de computadores diante do crescente papel dessas redes na sociedade contemporânea. A evolução tecnológica, que transformou a estrutura dos sistemas computacionais de uma abordagem centralizada para sistemas distribuídos, trouxe desafios substanciais, especialmente em relação à segurança. O objetivo principal da pesquisa é fornecer informações que auxiliem as corporações na mitigação de ameaças cibernéticas e aprimorem as estratégias de segurança existentes. A metodologia baseia-se em revisão bibliográfica, consolidando teorias e conceitos-chave de autores renomados.

Ao analisar a segurança de redes de computadores, destaca-se a relevância dos profissionais de segurança, que desempenham um papel vital na identificação, análise e resposta a vulnerabilidades e ameaças. Soluções como firewalls, sistemas de detecção/prevenção de intrusões e a promoção de uma cultura de segurança são abordadas como elementos essenciais na proteção contra ataques cibernéticos. A pesquisa identificou e explorou diversos tipos de ameaças, ressaltando a complexidade do cenário de segurança. A transição para sistemas distribuídos, junto ao aumento do uso da Internet, demanda investimentos críticos em segurança de redes. A aplicação de princípios fundamentais, como confidencialidade, integridade e disponibilidade, é crucial para preservar a segurança da informação.

Na apresentação dos resultados, destaca-se que a segurança em redes de computadores exige ações integradas, envolvendo tecnologias, ferramentas e uma cultura organizacional que valorize a segurança da informação. Profissionais qualificados desempenham papel crucial na identificação de vulnerabilidades, implementação de soluções de proteção e conscientização dos colaboradores.

A revisão bibliográfica desempenhou papel central na consolidação do conhecimento, contribuindo para inspirar organizações e futuros alunos do curso de Gestão da Tecnologia da Informação a aprimorar suas estratégias de segurança diante dos desafios em constante evolução no ambiente cibernético.

6 REFERÊNCIAS

ALMEIDA, M. B. Noções básicas sobre Metodologia de pesquisa científica. Universidade Federal de Minas Gerais. Disponível em: <https://mba.eci.ufmg.br/downloads/metodologia.pdf>. Acesso em 20 de outubro de 2023.

ALVES, Duly Thayna. Segurança em redes de computadores: tipos de ameaças, prevenções e soluções. 2021.

ANDRADE, João Paulo Moraes de. Contingência de risco: uma questão de segurança na preservação digital. 2018. Dissertação de Mestrado. Universidade Federal de Pernambuco.

Brasil. Tribunal de Contas da União. Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

CERVO, Amado Luis; BERVIAN, Antônio. Metodologia científica. 5. ed. São Paulo: Prentice Hall, 2002.

COSTA, Jonathan da Silva, et al. Segurança de Redes de Computadores na Internet. Revista Inova Ação, Teresina, v. 1, n. 2, art. 6, p. 77-88, jul./dez. 2012

DE OLIVEIRA, Mariane Pedrozo; MALAGOLLI, Guilherme Augusto. O impacto da tecnologia da informação na evolução dos serviços bancários. Revista Interface Tecnológica, v. 13, n. 1, p. 39-52, 2016.

GAVA, Marcela. Segurança Digital. Capterra, 2022. Disponível em: <https://www.capterra.com.br/blog/2155/seguranca−digital>. Acesso em: 3 de março de 2024.

HENKE, Márcia et al. Aprendizagem de máquina para segurança em redes de computadores: Métodos e aplicações. Sociedade Brasileira de Computação, 2011.

KAWAKANI, Cláudio Toshio. Segurança de computadores e aprendizado de máquina. Universidade Estadual de Londrina, LONDRINA-PR, 2014. Disponível em: <http://www.uel.br/cce/dc/wp-content/uploads/TCC-ClaudioKawakani-BCC-UEL-2014. pdf>. Acesso em: 22 de outubro de 2023.

MACEDO, Ricardo Tombesi et al. Redes de computadores. 2018.

MACHADO, Felipe Nery Rodrigues. Segurança da informação: princípios e controle de ameaças. Saraiva Educação SA, 2014.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. Hackers Expostos-: Segredos e Soluções para a Segurança de Redes. Bookman Editora, 2014.

MENEZES, Pablo Marques et al. Segurança em redes de computadores uma visão sobre o processo de Pentest. Interfaces Científicas-Exatas e Tecnológicas, v. 1, n. 2, p. 85-96, 2015.

MITSHASHI, Roberto Akio. Segurança de Redes, 2011. Disponível em: <http://www.fatecsp.br/dti/tcc/tcc0017.pdf>. Acesso em: 19 de outubro de 2023.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Lício. Segurança de redes em ambientes cooperativos. Novatec Editora, 2007.

SANTOS, Ivana. Segurança de rede no ambiente corporativo. 2023.

STALLINGS, William Criptografia e segurança de redes: princípios e práticas. 6. ed. – São Paulo: Pearson Education do Brasil, 2015.