AMEAÇAS E VULNERABILIDADES EM SISTEMAS E REDES: UMA ANÁLISE CIENTÍFICA BASEADA EM EVIDÊNCIAS RECENTES

Samuel De Lorenzi Ribeiro[1], Wesllen Felipe Langaro Raiser da Cruz[2], FABIANO DE OLIVEIRA WONZOSKI[3]

1. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
2. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
3. Docente do curso de graduação em Ciência de Computação, Unoesc, Videira, SC

Autor correspondente: Samuel De Lorenzi Ribeiro, samueldelorenziribeiro@gmail.com

Área: Ciências Exatas e Tecnológicas

Introdução: O estudo analisa as principais ameaças e vulnerabilidades em sistemas e redes, com foco em ataques como malware, phishing, ransomware, DDoS e engenharia social. A partir de uma revisão sistemática de artigos científicos recentes, identificou-se que credenciais fracas, softwares desatualizados, configurações inadequadas e ausência de criptografia são pontos críticos explorados por agentes maliciosos. São discutidas estratégias de mitigação, incluindo autenticação multifatorial, atualizações automatizadas, protocolos avançados de segurança para redes Wi-Fi e uso de tecnologias emergentes como Inteligência Artificial para detecção proativa de ameaças. A crescente dependência global de sistemas digitais, aliada ao aumento significativo de incidentes, reforça a importância de políticas organizacionais, educação contínua e conformidade com regulamentações como GDPR e LGPD para a construção de ecossistemas digitais resilientes. **Objetivo:** Analisar ameaças cibernéticas contemporâneas e as vulnerabilidades que as possibilitam, propondo estratégias de mitigação baseadas em evidências recentes. **Método:** Foi realizada uma revisão sistemática da literatura, seguindo as diretrizes de Kitchenham e Charters (2007), com abordagem qualitativa. Foram selecionados três artigos científicos e técnicos publicados entre 2023 e 2025, considerando relevância temática, atualidade e rigor metodológico. Os dados foram organizados em eixos temáticos (ameaças, vulnerabilidades, redes Wi-Fi) e analisados criticamente para identificar convergências e lacunas. **Resultados:** Malware representa 35% dos incidentes de segurança, explorando vulnerabilidades em softwares desatualizados ou configurações incorretas. Phishing responde por 80% dos vazamentos de dados, sendo potencialmente mitigado com filtros aprimorados por IA e treinamentos. Ransomware mantém alta incidência global, com proteção favorecida por backups isolados e controle de acesso restritivo. Ataques DDoS têm impacto significativo e podem ser mitigados com soluções baseadas em SDN. A engenharia social explora a psicologia humana, reforçando a importância da MFA e de uma cultura organizacional de segurança. Quanto às vulnerabilidades, destacam-se credenciais fracas, softwares sem atualização, configurações incorretas e ausência de criptografia, sendo recomendadas práticas como uso de gerenciadores de senhas, automação de patches, auditorias e adoção de protocolos seguros (WPA3, TLS 1.3). Para redes Wi-Fi, sugere-se segmentação de SSIDs e protocolos mais robustos, enquanto comunicações seguras podem ser fortalecidas com VPNs avançadas e criptografia resistente a ataques quânticos. **Conclusão:** As ameaças cibernéticas são multifacetadas e demandam soluções integradas que combinem tecnologias avançadas, boas práticas organizacionais e educação contínua. A segurança de redes e comunicações criptografadas constitui base essencial para a proteção de dados, enquanto a colaboração entre setores e investimentos em pesquisa são decisivos para enfrentar riscos emergentes, incluindo ataques baseados em computação quântica.

Palavras-chave: Segurança cibernética; Vulnerabilidades de rede; Malware.