VAZAMENTOS DE DADOS E ATAQUES CIBERNÉTICOS

Brayan Olivo FELIX[*]
João Roberto Domingos da SILVA[**]
José Henrique Pereira da SILVA[***]
Taires Sanches de CARVALHO[****]
Elaine Doro Mardegan COSTA[*****]

RESUMO

Introdução: Este trabalho examina os vazamentos de dados e ataques cibernéticos, ressaltando a necessidade de estratégias eficazes para sua prevenção, uma vez que há aumento de incidentes cibernéticos afetando governos, empresas e indivíduos e as consequências são significativas para a sociedade e a economia. **Objetivo:** Analisar os tipos mais comuns de vazamentos de dados e ataques cibernéticos para identificar processos e estratégias eficazes na prevenção desses riscos. **Metodologia:** Adotou-se a pesquisa exploratória e descritiva, sendo uma revisão bibliográfica de fontes científicas disponíveis no Google Acadêmico. **Resultados**: Com avanço do conhecimento em segurança cibernética exige-se soluções práticas para problemas reais que afetam diretamente a sociedade e a economia global. Quanto aos vazamentos de dados, cita-se *Phishing*, sendo ataques realizados por cibercriminosos que enganam usuários para obterem informações, senhas e dados financeiros com e-mails falsos; e, *Malware*, que são os *softwares* maliciosos, como vírus ou *ransomware*, que infectam sistemas e permitem o acesso não autorizado. Assim, é preciso o treinamento de Funcionários, sobre práticas seguras e reconhecimento de *phishing* e outras ameaças. Torna-se necessário o controle de acesso e a implementação do menor privilégio e uso de autenticação multifator. Para a proteção de informações a criptografia de dados pode evitar o acesso não autorizado. Também o uso de *Backups* frequentes e seguros ´podem garantir a recuperação em caso de perda ou ataque. Já o monitoramento de redes permitirá a resposta rapidamente a incidentes ou atividades suspeitas. **Conclusão:** a prevenção eficaz requer uma combinação de boas práticas, incluindo treinamento contínuo, controle de acesso com autenticação multifator, criptografia de dados e *backups* regulares. Além disso, é essencial manter monitoramento constante, aplicar atualizações de segurança, realizar auditorias periódicas e desenvolver um plano de continuidade de negócios para garantir uma recuperação rápida em caso de incidentes.

Palavras-chave: vazamentos de dados; segurança; privacidade.

[*] Discente do curso de Análise de Desenvolvimento de Sistemas do Centro Universitário de Santa Fé do Sul, SP – Unifunec, jp408011@gmail.com
[**] Discente do curso de Análise de Desenvolvimento de Sistemas do Centro Universitário de Santa Fé do Sul, SP – Unifunec, brayanofelix@gmail.com
[***] Discente do curso de Análise de Desenvolvimento de Sistemas do Centro Universitário de Santa Fé do Sul, SP – Unifunec. Joaoclashbrgames123@gmail.com
[****] Discente do curso de Análise de Desenvolvimento de Sistemas do Centro Universitário de Santa Fé do Sul, SP – Unifunec. tairessanshesdecarvalho@gmail.com
[*****] Docente do Centro Universitário de Santa Fé do Sul, SP – Unifunec. elamardegan@hotmail.com