Securing Third-Party Remote Access in Business Environments

Abstract

As digital interconnectivity expands, modern enterprises are increasingly dependent on third-party vendors and service providers who need remote access to internal systems for various functions, including maintenance and technical support. Although such access enhances operational workflows, it simultaneously presents critical cybersecurity challenges such as unauthorized data breaches, malware entry points, and regulatory non-compliance. This study seeks to analyze existing security measures employed by organizations to manage third-party remote access and uncover prevalent weaknesses. It will assess the role of advanced security approaches like Zero Trust Architecture, Multi-Factor Authentication (MFA), and network segmentation in mitigating these risks. The research methodology includes surveys and case studies of businesses leveraging third-party access, followed by a risk analysis and the formulation of actionable security recommendations. The anticipated outcome is a set of strategic guidelines and a robust framework to help organizations secure third-party access without compromising efficiency.