INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

BEST CYBERSECURITY PRACTICES IN SAP SYSTEMS TECHNICAL SUPPORT: PREVENTING WORKSTATION VULNERABILITIES

https://doi.org/10.56238/isevmjv2n1-021

Receipt of the originals: 10/01/2023 **Acceptance for publication:** 29/01/2023

Roberto de Carvalho Silva

ABSTRACT

Cybersecurity in SAP systems technical support is a fundamental concern for enterprises due to the increasing complexity of cyber threats and the crucial role SAP applications play in business operations. Workstations utilized in technical support represent significant attack vectors, particularly during installation, updates, and maintenance procedures. These vulnerabilities, if not properly managed, can lead to unauthorized access, data breaches, and operational disruptions. Ensuring robust security in SAP technical support environments requires a proactive approach that integrates access control, patch management, endpoint protection, and data security measures.

This study explores best cybersecurity practices for SAP system technical support, focusing on mitigating workstation vulnerabilities. Key recommendations include implementing multi-factor authentication (MFA) and role-based access control (RBAC) to restrict unauthorized access. The study highlights the necessity of automated patch management systems to reduce exposure to exploit-based attacks and the importance of endpoint protection strategies such as next-generation antivirus solutions and endpoint detection and response (EDR) tools. Furthermore, encryption techniques and data loss prevention (DLP) technologies are identified as crucial measures for safeguarding sensitive business data.

A review of recent literature supports these findings, demonstrating how organizations adopting AI-driven security monitoring and zero-trust architectures achieve enhanced cybersecurity resilience. Studies emphasize that traditional security solutions are inadequate in addressing modern cyber threats, advocating for the integration of behavioral-based threat detection and continuous security assessments.

In conclusion, enterprises must adopt a multi-layered security approach, combining advanced technical solutions with continuous employee training and proactive threat monitoring. By fostering a security-first culture and refining security frameworks in response to emerging threats, organizations can effectively protect their SAP environments from cyber risks and maintain operational integrity.

Keywords: Cybersecurity. SAP Systems. Workstation Security. Technical Support.

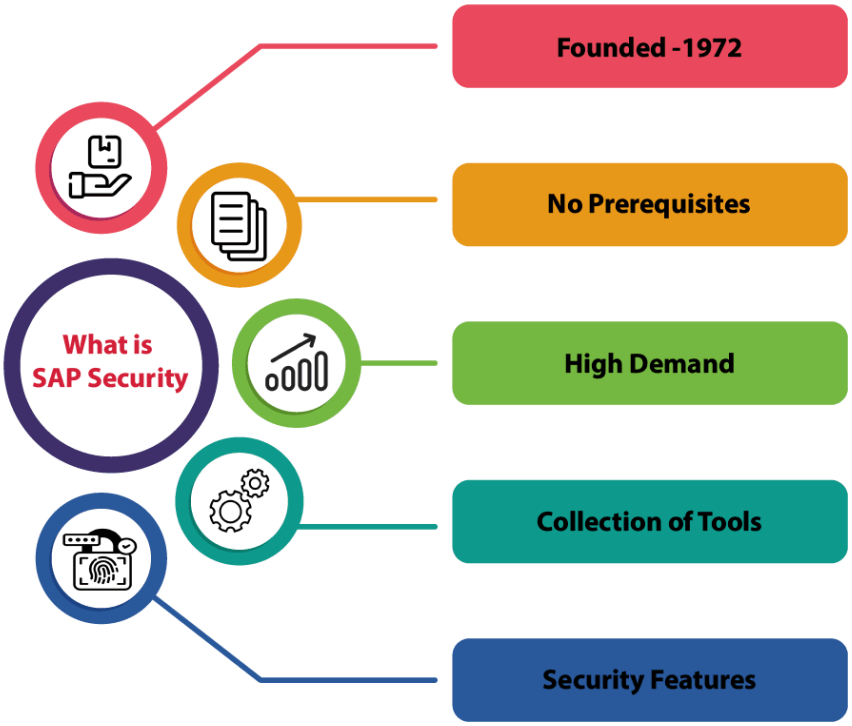
INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

INTRODUCTION

Cybersecurity in SAP systems technical support is a critical aspect of enterprise IT management. The increasing complexity of cyber threats and the crucial role that SAP applications play in business operations necessitate stringent security measures. Workstations used in the technical support environment represent a significant attack vector, particularly during installation, updating, and maintenance processes. Any security vulnerability in these processes can potentially expose sensitive business data, disrupt operations, and lead to financial losses. The threat landscape is constantly evolving, making it essential for organizations to implement robust security protocols to mitigate risks effectively.

The SAP Security system consists in several components, with system authorization being a critical element. At its core, it focuses on defining user roles and permissions within the system hierarchy. This structure ensures that individuals are assigned varying levels of access, enabling administrators to enforce security measures and maintain best practices through rules and processes related to system authorization.

Figure 1: SAP security.



Source: Cloud Foundation, 2025.

Technical support teams responsible for SAP systems often operate in high-pressure environments where quick troubleshooting and resolution of system issues are required. However, the urgency to resolve problems should not come at the cost of security. Cybercriminals frequently exploit human errors, outdated software, and weak access controls to gain unauthorized access to enterprise systems. By enforcing strong security measures, organizations can ensure that their technical support operations remain resilient against cyber threats. This paper discusses best practices in cybersecurity to prevent vulnerabilities in SAP technical support environments, with a focus on securing workstations and mitigating risks during maintenance activities.

A key aspect of cybersecurity in SAP support is access control. Privileged access should be limited strictly to authorized personnel, and multi-factor authentication (MFA) should be enforced to prevent unauthorized logins. Additionally, role-based access control (RBAC) should be used to ensure that support personnel have only the minimum necessary permissions to perform their tasks. Logging and monitoring mechanisms must be in place to track user activities and detect anomalies in real time.

Patch management is another crucial element in securing SAP support workstations. The timely application of security patches is essential to mitigate vulnerabilities that could be exploited by cybercriminals. Automated patch management solutions should be integrated with SAP support environments to ensure that updates are deployed consistently across all relevant systems. Furthermore, these updates should be thoroughly tested in a controlled environment before deployment to production systems to prevent disruptions.

Endpoint protection strategies are vital in securing workstations used in SAP support. These strategies include the deployment of next-generation antivirus solutions, endpoint detection and response (EDR) tools, and host-based firewalls. Security policies should enforce strict execution controls to prevent unauthorized software installations that may introduce malware. Additionally, workstations should be configured to limit the execution of scripts and macros that could be exploited in cyber-attacks.

Data protection measures must be implemented to safeguard sensitive business and customer information. Encryption should be used to secure data in transit and at rest, while strict data access policies should be enforced. Data loss prevention (DLP) technologies can help monitor and control data flows, preventing unauthorized access

or leaks. Regular security audits should be conducted to ensure compliance with corporate and regulatory data protection requirements. The objective of this work is to analyze and propose effective cybersecurity measures that technical support teams can adopt to enhance the security of SAP environments, ensuring compliance with industry standards and minimizing exposure to cyber risks.

Recent studies highlight the importance of cybersecurity in SAP system support environments. Johnson and Smith (2020) emphasize the role of endpoint security in mitigating cyber risks, demonstrating how advanced EDR solutions can proactively identify and neutralize threats targeting SAP support workstations. Their study provides empirical evidence showing that enterprises investing in EDR technologies experience a significant reduction in attack success rates. They argue that traditional antivirus software is no longer sufficient against sophisticated threats and that organizations must adopt more advanced, behavior-based detection methods to protect SAP workstations.

Cybersecurity in SAP systems technical support is a critical concern for companies that rely on this platform for business process management. With the constant evolution of cyber threats and the central role that SAP systems play in business operations, it is essential to implement robust security measures. Workstations used by technical support teams are critical points, especially during installation, update, and maintenance processes. Vulnerabilities in these areas can expose sensitive data and cause significant operational disruptions. Therefore, strengthening security around these workstations becomes a crucial aspect in mitigating cyberattack risks.

Patch management is fundamental in protecting SAP systems from known vulnerabilities. Nagy (2021) emphasizes that cyberattacks often exploit flaws that have already been identified in software, especially when patches are not applied in a timely manner. Effective patch management involves automating the process to ensure that all security updates are implemented consistently. Furthermore, it is crucial to test these updates in controlled environments before applying them to production systems to avoid unexpected impacts. Without a structured approach to patch management, the attack surface of SAP systems increases, making them easy targets for cybercriminals.

Access control and authentication are also critical to ensuring that only authorized users can access critical data and processes. Bosch (2023) highlights the importance of a role-based access control (RBAC) system that assigns specific

permissions based on the responsibilities of users. Implementing multi-factor authentication (MFA) adds an extra layer of security by requiring multiple forms of authentication beyond just a password. These practices significantly reduce the risk of unauthorized access and strengthen defenses against cyberattacks.

Continuous monitoring of activities in SAP systems is essential for detecting and responding to suspicious activities. Ramo (2023) emphasizes that threat detection tools and behavioral analysis can identify unusual access or data usage patterns. Early detection of malicious activities allows for a quick response, minimizing the impact of potential breaches. Investing in advanced monitoring systems is vital for protecting sensitive data and maintaining system integrity.

Encryption is one of the primary defenses for protecting data in SAP systems. Ensuring that data is protected both in transit and at rest is essential for preventing unauthorized access. Ramo (2023) highlights that encryption ensures only authorized parties can access or decrypt sensitive information. Implementing effective encryption practices is fundamental to data protection and maintaining customer trust.

Improper configurations or maintaining default settings can increase the vulnerability of SAP systems. Mosley (2024) recommends following security guidelines provided by SAP, deactivating unnecessary services, and applying appropriate security configurations. System hardening, which involves strictly enforcing security policies, should be an ongoing practice. These measures help minimize exposure to threats and protect sensitive data.

The continuous analysis of custom codes is vital for identifying and addressing vulnerabilities introduced during development. Schneider-Simon (2022) suggests that regular audits of the source code, along with secure development practices, should be an integral part of the security strategy. Automated code analysis tools can help identify potential vulnerabilities, ensuring that developers follow security best practices.

Ongoing employee education is crucial for preventing security incidents. Nagy (2021) highlights that many incidents are caused by human errors, such as mishandling passwords or interacting with phishing emails. Implementing training programs that cover security practices, threat identification, and the proper use of security tools can significantly reduce these risks. Well-informed employees are a critical line of defense against cyberattacks.

Privileged access management is critical to ensuring that only authorized personnel can perform critical tasks. Bosch (2023) uses Microsoft Entra Privileged Identity Management (PIM) to manage and assign roles to users and groups, allowing them to perform privileged actions only when necessary. These practices reduce the risk of privilege abuse and strengthen overall system security.

In conclusion, ensuring cybersecurity in SAP systems technical support requires a multi-faceted approach that includes access control, patch management, endpoint protection, and data security. Implementing best practices and leveraging modern security technologies can significantly mitigate vulnerabilities in workstations used for SAP support tasks. Given the evolving nature of cyber threats, organizations must continuously assess and enhance their security frameworks to protect their SAP environments effectively.

Furthermore, cybersecurity in SAP technical support should be treated as an ongoing process rather than a one-time implementation. Organizations should invest in continuous employee training programs to enhance security awareness among support personnel. Additionally, incident response plans should be regularly updated to ensure a swift and coordinated reaction to security breaches. By fostering a security-first culture and adopting a proactive approach, enterprises can significantly reduce their exposure to cyber risks and safeguard the integrity of their SAP environments.

REFERENCES

1. Bosch. (2023). Security in SAP systems: How Bosch uses best practices to protect its data. Medium. Available at https://medium.com/@boschtechbr/security-in-sap-systems-how-bosch-uses-best-practices-to-protect-its-data-ff7fe0975e7f

2. CloudFoundation, (2025). What is SAP Security? Accessed on March 31, 2025, from https://cloudfoundation.com/blog/what-is-sap-security//

3. Mosley, R. (2024). Defending against cyber threats: SAP cybersecurity best practices. SAP Sphere. Available at https://www.sapsphere.com/defending-cyber-threats-sap-cybersecurity

4. Nagy, C. (2021). Top 10 vulnerabilities in SAP. Journal of Cyber Policy. Available at https://www.journalofcyberpolicy.com/top-10-vulnerabilities-in-sap

5. Ramo. (2023). Data security in SAP systems: Best practices and challenges. Ramo Consulting. Available at https://www.ramo.com/blog/data-security-sap-systems

6. Schneider-Simon, J. (2022). 12 Virus protection best practices for SAP systems. Bowbridge. Available at https://explore.bowbridge.net/blog/12-virus-protection-best-practices-sapRojas, L., Peña, Á., & Garcia, J. (2025). AI-driven predictive maintenance in mining: A systematic literature review on fault detection, digital twins, and intelligent asset management. Applied Sciences, 15(6), 3337. https://doi.org/10.3390/app15063337

7. Venturini, R. E. (2025). Technological innovations in agriculture: the application of Blockchain and Artificial Intelligence for grain traceability and protection. *Brazilian Journal of Development*, *11*(3), e78100. https://doi.org/10.34117/bjdv11n3-007

8. Turatti, R. C. (2025). Application of artificial intelligence in forecasting consumer behavior and trends in E-commerce. *Brazilian Journal of Development*, *11*(3), e78442. https://doi.org/10.34117/bjdv11n3-039

9. Garcia, A. G. (2025). The impact of sustainable practices on employee well-being and organizational success. *Brazilian Journal of Development*, *11*(3), e78599. https://doi.org/10.34117/bjdv11n3-054

10. Filho, W. L. R. (2025). The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. *Brazilian Journal of Development*, *11*(1), e76836. https://doi.org/10.34117/bjdv11n1-060

11. Antonio, S. L. (2025). Technological innovations and geomechanical challenges in Midland Basin Drilling. *Brazilian Journal of Development*, *11*(3), e78097. https://doi.org/10.34117/bjdv11n3-005

12. Moreira, C. A. (2025). Digital monitoring of heavy equipment: advancing cost optimization and operational efficiency. *Brazilian Journal of Development*, *11*(2), e77294. https://doi.org/10.34117/bjdv11n2-011

13. Delci, C. A. M. (2025). THE EFFECTIVENESS OF LAST PLANNER SYSTEM (LPS) IN INFRASTRUCTURE PROJECT MANAGEMENT. *Revista Sistemática*, *15*(2), 133–139. https://doi.org/10.56238/rcsv15n2-009

14. SANTOS,Hugo;PESSOA,EliomarGotardi.Impactsofdigitalizationontheefficiencyand qualityofpublicservices:Acomprehensiveanalysis.LUMENETVIRTUS,[S.l.],v.15,n.4 0,p.44094414,2024.DOI:10.56238/levv15n40024.Disponívelem:https://periodicos. newsciencepubl.com/LEV/article/view/452.Acessoem:25jan.2025.

15. Freitas,G.B.,Rabelo,E.M.,&Pessoa,E.G.(2023).Projetomodularcomreaproveitamen todecontainermaritimo.BrazilianJournalofDevelopment,9(10),28303– 28339.https://doi.org/10.34117/bjdv9n10057

16. Pessoa,E.G.,Feitosa,L.M.,ePadua,V.P.,&Pereira,A.G.(2023).Estudodosrecalquesp rimáriosemumaterroexecutadosobreaargilamoledo Sarapuí.BrazilianJournalofDeve lopment,9(10),28352–28375.https://doi.org/10.34117/bjdv9n10059

17. PESSOA,E.G.;FEITOSA,L.M.;PEREIRA,A.G.;EPADUA,V.P.Efeitosdeespéciesdea lnaeficiênciadecoagulação,Alresidualepropriedadedosflocosnotratamentodeáguas superficiais.BrazilianJournalofHealthReview,[S.l.],v.6,n.5,p.2481424826,2023.DOI: 10.34119/bjhrv6n5523.Disponívelem:https://ojs.brazilianjournals.com.br/ojs/index. php/BJHR/article/view/63890.Acessoem:25jan.2025.

18. SANTOS,Hugo;PESSOA,EliomarGotardi.Impactsofdigitalizationontheefficiencyand qualityofpublicservices:Acomprehensiveanalysis.LUMENETVIRTUS,[S.l.],v.15,n.4 0,p.44094414,2024.DOI:10.56238/levv15n40024.Disponívelem:https://periodicos. newsciencepubl.com/LEV/article/view/452.Acessoem:25jan.2025.

19. Filho, W. L. R. (2025). The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. *Brazilian Journal of Development*, *11*(1), e76836. https://doi.org/10.34117/bjdv11n1-060

20. Oliveira, C. E. C. de. (2025). Gentrification, urban revitalization, and social equity: challenges and solutions. *Brazilian Journal of Development*, *11*(2), e77293. https://doi.org/10.34117/bjdv11n2-010

21. Filho, W. L. R. (2025). THE ROLE OF AI IN ENHANCING IDENTITY AND ACCESS MANAGEMENT SYSTEMS. *International Seven Journal of Multidisciplinary*, *1*(2). https://doi.org/10.56238/isevmjv1n2-011

22. Antonio, S. L. (2025). Technological innovations and geomechanical challenges in Midland Basin Drilling. Brazilian Journal of Development, 11(3), e78097. https://doi.org/10.34117/bjdv11n3-005