LAYER SEVEN SECURITY

PROTECTING SAP SYSTEMS FROM RANSOMWARE

PROTECTING SAP FROM RANSOMWARE

Ransomware is one of the most significant threats to organizations today. It is a form of cybercrime through which criminals remotely compromise and encrypt computer systems and demand a ransom in return for restoring or not exposing sensitive data. Ransomware attacks increased by 139% between 2019 and 2020, impacting all industries and sectors. The average downtime from a ransomware attack is 21 days. Full recovery from an attack takes an average of 287 days.

Tackling ransomware is challenging. Cybercriminals are often based in countries that are unable or unwilling to prosecute the threat actors. Ransom payments performed through cryptocurrency are difficult to trace. The malware strains used to execute attacks are constantly evolving. For this reason, organizations should develop clear, actionable frameworks for ransomware mitigation, response and recovery.

This guide provides a framework for securing SAP systems against ransomware. SAP applications are built for high availability. They must be continually accessible to support the mission-critical operations and strategic objectives of organizations. Ransomware attacks that interrupt the availability of these applications can have a devastating impact on organizations.

Ransomware can target SAP applications through vulnerable operating systems. However, securing SAP hosts alone will not prevent ransomware exploits impacting SAP systems. Attackers can exploit the trust relationship between SAP applications and underlying operating systems to perform privileged OS commands through the application layer. Since the commands are performed using the privileges of the SAP OS user through application functions, the exploits will not draw attention and will therefore avoid detection.

The guide provides specific recommendations across four areas: Identification, Prevention, Detection and Restoration. It includes practical steps for hardening SAP systems and detecting and responding to potential ransomware exploits. The framework significantly lowers the likelihood of a successful ransomware attack and increases the probability of a rapid recovery.

PROTECTING SAP FROM RANSOMWARE

| IDENTIFY

Identify and prioritize critical applications using the Landscape Management Database (LMDB) in SAP Solution Manager. The LMDB is the repository of system information in SAP landscapes. It includes software, database, host and network information for SAP systems. It can also include details such as impacted business units and the physical location of systems. Attributes in the LMBD should be used to tag mission-critical systems and register the contact information of key IT and business groups that should be included in the recovery process for a ransomware attack.

| PREVENT

Encrypt and authenticate SAP communications using SNC for SAP protocols and TLS for web-based protocols. Secure RFC, web services and other cross-system interfaces using UCON, SACF, and whitelists. Block external program starts in the gateway server. Authorizations for OS commands and other administrative privileges should be restricted. This includes RSBDCOS0, SM49 and CG3Z which can be used to download, install and run ransomware tools. Secure custom ABAP, UI5, Java and SQLScript programs that may be exploited to perform arbitrary OS commands. Reduce the attack surface by disabling vulnerable services including ICF services such as SOAP RFC and WEB RFC. Also disable vulnerable OS services including RDP and SMB. Stay up to date with SAP security patches using SAP Solution Manager.

| DETECT

Monitor OS command logs for sensitive commands including wget and bash. Also monitor gateway server logs for the execution of dangerous external programs. Detect sensitive URL calls using the HTTP log and Java trace logs. Investigate suspicious report and transaction starts and privileged actions captured in event logs. Monitor root commands and Sudo actions in SAP hosts and the creation and execution of OS files. Monitoring and alerting for indicators of compromise in SAP and OS logs can be performed using SAP Solution Manager. Alerts should be integrated from Solution Manager with SIEM systems for centralized monitoring and event correlation.

| RESTORE

Perform daily operating system and database backups to support the restoration of SAP systems. Backups should be stored in secondary locations. Define objectives for recovery points and recovery times for each system. Assign responsibilities for system recovery and document recovery procedures. Regularly test offline backups and restoration procedures. Activate alerts for backup failures using SAP Solution Manager..

LAYER SEVEN SECURITY

Layer Seven Security is an industry-leader in cybersecurity solutions and services for SAP. The organization is an SAP partner and recognized as one of the Top 25 Cybersecurity Companies 2020, Top 10 Vulnerability Management Solution Providers 2021, and Top Threat Intelligence Solution Providers 2023.

Cybersecurity Extension for SAP

The Cybersecurity Extension for SAP automates vulnerability management, threat detection, and incident response to secure SAP solutions against advanced persistent threats. The SAP-certified addon provides integrated security to protect SAP systems against ransomware across application, database and host layers. It supports cloud and hybrid SAP systems including S/4HANA, HANA, ABAP and J2EE platforms.

CONTACT US

www.layersevensecurity.com
info@layersevensecurity.com