CyberArk Publishes Steps to Implement NIST 800-53 Controls and Continuous Monitoring with a Special Focus on Privileged Account Management

November 3, 2011 4:28 PM ET

Whitepaper Outlines the Recommended Security Controls for Federal Information Systems and Organizations and Related Steps Toward Gaining FISMA Compliance

NEWTON, Mass. - November 3, 2011 - CyberArkÂ® Software, the leading global information security provider for protecting and managing critical applications, identities and sensitive information, today released an informative whitepaper for federal agencies, â€œComplying with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.â€With a special focus on establishing a proactive, preventative approach to privileged account management, the paper details how to implement the necessary controls described within NIST 800-53 to achieve FISMA compliance.

NIST 800-53 provides federal information systems and agencies with the recommended security controls to ensure ongoing situational awareness of the security of their IT systems. CyberArkâ€™s whitepaper was developed in conjunction with the increased focus that NIST 800-53 has placed on instilling controls to combat insider threats and the abuse of privileged accounts, while drawing attention to some of the shortcomings of traditional encryption-based approaches. In particular, it focuses on steps organizations can take to better manage across the privileged account management lifecycle, gain better control over shared accounts and institute real-time continuous monitoring solutions as part of a comprehensive risk management framework.

An Overview of Primary Security Controls and the Privilege Connection
While some aspects of Privileged Identity Management may be addressed procedurally, the majority of the necessary security controls outlined in NIST 800-53â€™s recommendations require a dedicated solution for the proactive management and audit of privileged users. CyberArkâ€™s Privileged Identity Management Suite and Privileged Session Management Suite enable an organization to execute the following controls to securely provide users and applications with the privileges needed in order to complete their role - and their role only:

Access Control:
As the foundation for the management of users and accounts, this control addresses the creation and assignment of privileges. According to NIST 800-53â€™s recommendations, particular attention must be paid to privileged accounts and their elevated access rights to the sensitive information stored in a variety of information systems. CyberArk emphasizes the importance of controlling access across the privileged account lifecycle, encompassing steps for auto-discovery, management, policy definition and monitoring.

Audit and Accountability:
As NIST 800-53 suggests, this set of controls is critical when establishing a proactive approach to audit compliance and accountability. As detailed in the guidelines, auditable information must be available on demand. Without these built-in controls to continuously access sensitive information, log and monitor privileged actions, organizations will sacrifice accountability and fail to satisfy compliance requirements. CyberArkâ€™s Digital Vault provides tamper proof audit and log retention which is critical for ensuring the authenticity and safe keeping of all privileged audit information.

Identification and Authentication:
This control, according to NIST 800-53, asserts that â€œthe information system uniquely identifies and authenticates organizational users.â€This is especially critical for privileged and shared accounts - commonly utilized among the IT staff, diminishing an organizationâ€™s accountability while exposing password vulnerabilities. This control will establish a more effective password management program and accountability for shared accounts.

â€œWith each release, NIST guidelines detail the most critical security controls that must be implemented to mitigate security vulnerabilities. With NIST 800-53, it is clear that privileged account management is moving to the top of the risk assessment priority list for many organizations,â€• said Adam Bosnian, Executive Vice President, Americas and Corporate Development, CyberArk Software. â€œCombining the negative financial impact associated with non-FISMA compliance with rising internal and external threat awareness in the federal sector, this whitepaper provides specific advice organizations can use to enhance existing security solutions through policy-based automation and enhanced security controls around privileged account management.â€•

The NIST 800-53 whitepaper also describes applicable CyberArk solutions to establish NIST 800-53 controls through a preventative approach to information security. CyberArk provides several federal agencies with industry-leading solutions that protect critical assets, identify potential security vulnerabilities and mitigate risks by proactively managing and monitoring privileged accounts and activities.

About CyberArk

CyberArkÂ® Software is a global information security company that specializes in protecting and managing privileged users, applications and sensitive information to improve compliance, productivity and protect organizations against insider threats and advanced external threats. With its award-winning Privileged Identity Management, Sensitive Information Management and Privileged Session Management Suites, organizations can more effectively manage and govern data center access and activities, whether on-premise, off-premise or in the cloud, while demonstrating returns on security investments. CyberArk works with more than 900 global customers, including more than 35 percent of the Fortune 100. Headquartered in Newton, Mass., CyberArk has offices and authorized partners in North America, Europe and Asia Pacific.

For more information, visit www.cyberark.com.

Thursday, November 3, 2011 - 14:15