CyberArk Global Security Survey: Privileged Account Exploitation the Common Link in Enterprise Assaults

June 12, 2012 4:44 PM ET

71 Percent Cite Insider Threat as Primary Security Risk; 64 Percent Recognize the Privileged Connection in High Profile Breaches such as RSA, Global Payments and US Chamber of Commerce

NEWTON, Mass. and LONDON - June 12, 2012 - According to the results of CyberArkÂ® Softwareâ€™s annual global IT security survey, businesses recognize that the exploitation of privileged account access played a prominent role in most of the worldâ€™s most notorious data breaches. The 6th Annual â€œGlobal Trust, Security and Passwords Surveyâ€ is a result of interviews with 820 IT managers and C-level professionals across North America and EMEA, primarily from enterprise-class companies.

Analysis of the survey highlights that as the enterprise perimeter dissolves and reports of internal and external threats increase, privileged access points have become the primary target for all enterprise attacks. Privileged access points consist of privileged and administrative accounts, default and hardcoded passwords, application backdoors, and more. These accounts act as a gateway to an organizationâ€™s most sensitive data, which is accessible across systems, applications and servers. Key findings of the survey include:

- Privileged accounts are increasingly being targeted in enterprise-assaults - regardless of the attack entry point :
- 71 percent of respondents consider insider threats to be the greatest security risk to their organization; 29 percent cite external threats, including targeted cyber-attacks and opportunistic hacks.
- 64 percent of respondents believe that the majority of recent security attacks have involved the exploitation of privileged account access.

Recent high-profile security attacks, such as the RSA and Global Payments data breaches, have made an impact on security strategies this year:
When asked if they were rethinking security strategies based on these high profile breaches, more than half said yes (51 percent)
Respondents were asked to rank their 2012 IT security priorities in order of importance:

- Vulnerability Management (17 percent); Privileged Identity Management (16 percent); Security Information and Event Monitoring (SIEM) (15 percent); Anti-virus/malware (13 percent).

Despite the growing awareness of the privileged connection in cyber-attacks and the growing insider threat, some businesses are failing to uphold their responsibility for securing customer and similar sensitive information:

- 43 percent of respondents stated that their organizations do not monitor the use of privileged accounts or were unsure of whether they did.
- Of those organizations that monitor privileged access 52 percent of respondents believe they can get around the current controls.
- Current legislative and regulatory efforts to curb data breaches have proven ineffective to date:
- When asked if data breach notification laws are effective in curbing data loss, 72 percent of respondents stated no, while only 28 percent stated yes.

The perception of the insider threat as the greatest security risk is driven by continued unauthorized access to sensitive information:

- 45 percent of respondents indicated that they have access to information on a system that was not relevant to their role.
- 42 percent of respondents indicated that they or a colleague have used admin passwords to access information

that was otherwise confidential; 25 percent of respondents were unsure.

- 55 percent of respondents believe that competitors have received their companyâ€™s highly sensitive information or intellectual property.

Supporting Quote
â€œWhether itâ€™s a malicious insider looking to steal information, or an external attacker looking to exploit privileged accounts to gain access to the network and sensitive information, itâ€™s clear that privileged access points have emerged as the priority target of enterprise cyber-assaults. This pattern has been demonstrated in some of the most high profile attacks, including Global Payments, Utah, and even with the recent Flame virus,â€ said Udi Mokady, founder and CEO of CyberArk. â€œEverything that weâ€™ve known about security is changing - itâ€™s no longer acceptable to simply focus on the perimeter and hope to keep attackers out. Businesses need to start with the assumption that the attackers are already on the inside and focus internal security structures to safeguard the access points to sensitive data. Controlling privileged access points needs to be a priority and should be considered a corporate responsibility.â€

Full Research Brief: 2012 Trust, Security & Password Report
Twitter: @CyberArk
LinkedIn: http://www.linkedin.com/groups/Privileged-Identity-Management-3663453/about

About CyberArk

CyberArkÂ® Software is a global information security company that specializes in protecting and managing privileged users, sessions, 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 nearly 1000 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, please visit www.cyberark.com.

Tuesday, June 12, 2012 - 14:45