CyberArk Survey Shows Majority of Organizations Underestimate Scope of Privileged Account Security Risk

May 8, 2013 4:10 PM ET

Despite Best Practices, Organizations Failing to Secure Primary Attack Target for Cyber-Attackers; More than Half of All Businesses Share Privileged Account Access Internally

NEWTON, Mass. - May 8, 2013 - Despite repeated warnings, a majority of organizations are failing to enact recommended best practice security policies around one of the primary targets of advanced attacks â€" privileged accounts. According to the results of **CyberArk Software's** global IT security survey on Privileged Account Security & Compliance, 86 percent of large enterprise organizations either do not know or have grossly underestimated the magnitude of their privileged account security problem, while more than half of them share privileged passwords internally. The Privileged Account Security & Compliance Survey 2013 is a result of interviews with 236 IT managers and C-level professional across North America and EMEA, primarily from enterprise-class companies. The full report can be downloaded **here**.

Privileged accounts have emerged as the primary target for **advanced enterprise attacks** and have been exploited to perpetrate some of the most devastating cyber-attacks and data breaches in recent memory, including those occurring at Saudi Aramco, South Korea, Global Payments, the South Carolina Department of Revenue, and the U.S. Department of Energy among others. According to a recent report by information security firm Mandiant, "APT intruders prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts."[1]

Privileged accounts consist of privileged and administrative accounts, default and hardcoded passwords, application backdoors, and more. These accounts act as a gateway to an organization's most sensitive data, which is accessible across systems, applications and servers. Despite the repeated abuse of privileged accounts in cyber-attacks, organizations continue to have a difficult time identifying and managing these critical vulnerabilities.

Key findings of the survey include:

- **Organizations Failing to Accurately Scope the Privileged Problem**
  - Based on the examination of more than 1200 customer deployments, CyberArk determined that the number of privileged accounts in an organization is typically 3-4 times the number of employees. When asked to estimate the number of privileged accounts in their organization, 86 percent of respondents from large enterprises (5000+ employees) stated they either didn't know how many accounts they had or that they had no more than 1 per employee. That means at least 2 out of every 3 privileged accounts in these organizations are either unknown or unmanaged.
  - Privileged accounts can be found in any device with a microprocessor, including PCs, databases, networked devices like copiers, operating systems and more. When asked where privileged accounts could be found, 63 percent correctly stated 'all of the above.' This means that 37 percent of respondents do not understand where privileged accounts exist in their organization.

- **Shared Vulnerabilities â€" Businesses Sharing Privileged Passwords Despite Best Practices**
  - Fifty one percent of all organizations surveyed stated that privileged and administrative account passwords were shared among "approved" users.
  - The problem is more wide spread among large enterprises, where 56 percent of respondents stated they shared privileged passwords, as opposed to 47 percent of SMBs (5000 employees or less).
  - According to Gartner's "Ten Best Practices for Managing Privileged Accounts," the passwords for 'shared privileged accounts' should never be shared, stating "Ã¢â‚¬Â¦sharing super-user account passwords dramatically increases the risk that a password may become known outside the intended groups. Furthermore, poorly controlled use of shared accounts cannot provide the individual accountability that is a security best

practice and demanded by regulatory compliance."[2]

- **Changing Privileged Passwords â€" Change Frequency Below Recommended Standards**
  - Despite 82 percent of respondents stating they have processes in place for changing privileged passwords, 49 percent of all businesses take 90 days or longer to change their privileged passwords, while 74 percent take 60 days or longer. This problem is exacerbated with large enterprises, where 53 percent take 90 days or longer to change privileged passwords.
  - While some industry standards suggest that privileged account passwords be changed "at a frequent interval of no longer than 90 days," the recent spate of attacks using privileged accounts demonstrates this time period is no longer sufficient and leaves organizations vulnerable. Privileged account password changes should be automated and restricted to one-time use to ensure tighter security standards.

Supporting Quote:

"It has become clear that privileged accounts are a priority target for cyber-attackers â€" every new report highlights this and every new attack reveals the privileged pathway the attackers are travelling. Despite this, organizations are having a difficult time understanding the magnitude of this security problem in their environments because privileged accounts exist everywhere," said John Worrall, CMO of CyberArk. "To minimize the risk associated with these accounts, organizations need to identify where these accounts exist, control access to them, and monitor exactly what is being done with them. Implementing a privileged account security solution to automate these processes helps organizations enforce these controls, while providing a clear audit trail for accountability and security."

Full Research Brief: **http://goo.gl/EZJu3**

Twitter: **@CyberArk**

Free Privileged Account Security Risk Assessment: **http://www.cyberark.com/discover-dna**

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**, **Privileged Session Management** and**Sensitive Information 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 1,200 customers, including more than 40 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**.

CYBERARK

Wednesday, May 8, 2013 - 12:00