Privileged Accounts Emerge as Primary Enterprise Security Attack Vector; Drives Global Demand for CyberArk Solutions

May 29, 2012 4:45 PM ET

Regardless of Attacker Entry Point, High Profile Breaches Increasingly Share the Privileged Connection
NEWTON, Mass. - May 29, 2012 - The exploitation of privileged accounts has emerged as the primary attack vector for enterprise cyber-security assaults and played a significant role in the most devastating data breaches and enterprise attacks over the past two years.

As the enterprise perimeter dissolves, and reports of internal and external threats increase, privileged access points have become the primary target for 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.

The privileged connection among these attacks has resulted in a record number of enterprise customers turning to Cyber-ArkÂ® Software to better protect critical, and often unguarded, access points that lead to high value targets such as customer data and intellectual property. As a result, the company experienced more than 30 percent year over year revenue growth in 2011, and now has more than 1,000 global enterprise customers.

Recent industry data on popular attack vectors confirms this growing trend:

In March 2012, the Verizon Data Breach Investigation Report highlighted that several of the primary attack vectors used by hackers had a privileged connection. The report showed that the hacking methods used by percent of breaches within the hacking domain included:

- 55 percent were the result of exploitation of default or guessable credentials
- 40 percent used stolen login credentials
- 29 percent used brute force and dictionary attacks (indicative of weak passwords)

A recent Microsoft Intelligence Report highlighted that the Conficker worm was detected approximately 220 million times worldwide in the past two and a half years. Research shows that 92 percent of Conficker infections were a result of weak or stolen passwords.

Attackers have used the privileged pathway to perpetrate some of the most spectacular breaches over the past couple of years, including:

- United States Chamber of Commerce - Attackers bypassed the Chamberâ€™s perimeter security through simple spear phishing attacks, duping an employee into opening a document with spyware. The attackers then used this foothold to obtain administrator passwords, providing access to the entire network. Itâ€™s believed that the attackers had access to the network for more than a year before the breach was uncovered.
- Global Payments Data Breach - While the company has yet to release full details on the breach, analyst reports indicate that â€œattackers took over an administrative account that was not protected sufficiently.â€ The Wall Street Journal recently reported that up to seven million credit card accounts may be vulnerable.
- Utah Department of Health - Attackers were able to breach the organizationâ€™s servers by exploiting a default password. Personal medical records for more than 780,000 residents have been stolen.

â€œThe trends are clear and have been for some time. The entry points into a network are through simple means - spear phishing, malware, zero-day exploits - this is easily accomplished because the perimeter as we knew it fails to exist. But

once inside, attackers are increasingly targeting privileged accounts to gain widespread network access,â said Adam Bosnian, executive vice president Americas and corporate development, Cyber-Ark Software. â€œPrivileged access points are the keys to an organizationâ€™s most sensitive assets. Unfortunately, these accounts are often protected by weak or default passwords, which are seldom replaced. Businesses that are not securing and managing these high value targets are failing to uphold their responsibility for securing customer and similar sensitive information.â

For more information on recent attacks and the privileged connection, download Cyber-Arkâ€™s Infographic here: http://www.cyberark.com/ebooklanding/infographic.html

Twitter: @CyberArk
LinkedIn: http://www.linkedin.com/groups/Privileged-Identity-Management-3663453/about

About Cyber-Ark

Cyber-ArkÂ® 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. Cyber-Ark works with nearly 1000 customers, including more than 35 percent of the Fortune 100. Headquartered in Newton, Mass., Cyber-Ark has offices and authorized partners in North America, Europe and Asia Pacific. For more information, please visit www.cyberark.com.

Tuesday, May 29, 2012 - 14:30