Privileged Accounts Remain Most Coveted Target for Cyber-Attackers

November 20, 2012 4:04 PM ET

Analysis of Recent High Profile Cyber-Attacks Identifies Common Attack Vector â€" Privileged Accounts
NEWTON, Mass. - November 20, 2012 - Despite repeated warnings, organizations are still failing to lock down the primary target of most cyber-attacks â€" privileged access points. Cyber-Ark labs analyzed a string of recent, high-profile cyber-attacks, including the malware attack against Saudi oil giant Aramco and the Subway restaurant breach, and concluded that the common denominator of each breach was the exploitation of privileged access points.

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. Cyber-attackers continue to breach the corporate perimeter through common means â€" including phishing attacks, malware infected attachments, social media viruses, and other methods. Once inside, cyber-attackers infiltrate privileged access points to gain access to additional servers, databases and other high value systems.

According to a Gartner Research report on advanced persistent threats, protecting against this type of threat requires locking down privileged accounts. The report concluded that "to reduce the impact of social engineering attacks, ensure that end users do not have administrative access; and when IT administrator access is required for system administration, perform these functions on isolated systems that are not used for email or Web browsing."

Privileged accounts have served as the root cause of some of the most significant breaches in recent months, including:

- The Flame Virus â€" Flame, a virus considered the 'mother of all cyberweapons', had a sniffer component that scans traffic on an infected computer's local network, collecting usernames and passwords. From here, attackers were able to hijack administrative accounts and acquire high-level privilege to other computers and network locations
- Saudi Aramco â€" The New York Times recently reported that 'what is regarded as among the most destructive acts of computer sabotage on a company to date' was traced to an insider with privileged access to the Saudi state-owned oil company's computers.
- Subway Data Breach â€" In New Hampshire, two men plead guilty to stealing payment information from Subway restaurants and according to the court documents, the men "remotely scanned the Internet to identify POS systems with remote desktop software applications on them. They logged into the systems over the internet and cracked the passwords to gain administrative access." Once they gained access, they simply installed key logging software to capture data being input.

"For years, the discussion on securing privileged access points focused mostly on the insider threat and ensuring that only the properly credentialed had access to these power accounts. Sophisticated cyber-attackers understand the power and wide ranging access these accounts provide â€" which is why they continue to be the number one target in the majority of cyber-attacks," said Adam Bosnian, executive vice president Americas, Cyber-Ark Software. "Unsecured critical access points are a threat to all sensitive corporate data and systems and represent the greatest security challenge most businesses will face. Identifying all privileged access points and locking them down should be a priority for any security and compliance conscious executive."

Twitter: @CyberArk
LinkedIn: http://www.linkedin.com/groups/Privileged-Identity-Management-3663453/about
Download the Cyber-Ark security survey: http://goo.gl/oR2F2

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 more than 1,100 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, November 20, 2012 - 15:00