Global Survey: NSA, Retail Breaches Influenced Corporate Security Strategies the Most

July 28, 2014 2:45 PM ET

The Majority of Organizations Cite Privileged Account Takeover as the Most Difficult Stage of an Attack to Detect, Respond and Remediate

Newton, Mass. â€“ July 28, 2014 â€“ Sixty eight percent of businesses stated that the NSA breach by Edward Snowden and the number of retail/point of sale (PoS) system breaches in the past year were the most impactful in terms of changing security strategies to protect against the latest threats. The findings are part of CyberArkâ€™s 8th Annual Global Advanced Threat Landscape survey â€“ developed through interviews with 373 C-level and IT security executives across North America, Europe and the Asia-Pacific. The full survey can be downloaded for free here.

The majority of organizations surveyed believe that attacks reaching the privileged account takeover stage are the most difficult to detect, respond to and remediate. While the NSA breach is widely regarded as the prototypical insider-based attack, and the retail/PoS breaches are regarded similarly for outside attacks, the critical link between both attacks was the compromise and exploitation of privileged credentials.

Key findings of the 2014 survey include:

Snowden and Retail/PoS Breaches Influence Security Strategies the Most

- When asked which cyber-attacks or data breaches in the past year had the biggest impact on their businessâ€™ security strategy:
  - 37 percent of respondents cited the NSA/Edward Snowden breach
  - 31 percent of respondents cited the retail/PoS attacks
  - 19 percent of respondents cited government-sponsored espionage

Third-Party Privileged Access Emerges as Critical Security Vulnerability

- As companies move to the cloud and streamline the supply chain by providing routine network access to third-parties, cyber-attackers are increasingly targeting these partners to steal and exploit their privileged access to the target companyâ€™s network. This pathway was used in some of the most devastating breaches in the last 12 months. The survey found:
  - 60 percent of businesses now allow third-party vendors remote access to their internal networks
  - Of this group, 58 percent of organizations have no confidence that third-party vendors are securing and monitoring privileged access to their network

Attackers are on the Inside â€“ Protect Your Privileges

- Organizations continue to face sophisticated and determined attackers seeking to infiltrate networks. Many organizations face daily perimeter-oriented attacks, such as phishing, designed to give attackers a foothold to steal the privileged credentials of an employee to give them defacto insider status. The survey found:
  - 52 percent of respondents believe that a cyber-attacker is currently on their network, or has been in the past year
  - 44 percent believe that attacks that reach the privileged account takeover stage are the most difficult to detect, respond to and remediate; 29 percent believe it is the malware implantation stage

Other Findings of Note

- Survey respondents stated that the following trends were the most impactful in terms of shaping and changing security strategies:

    - 30 percent stated Bring Your Own Device (BYOD)
    - 26 percent stated cloud computing
    - 21 percent stated regulatory compliance
    - 6 percent stated the Internet of Things (IoT)
- When asked whether their organization had or was considering deploying security analytics, this yearâ€™s survey found that:
    - 31 percent of businesses have already deployed security analytics in some form
    - 23 percent were planning on deploying security analytics in the next 12 months
    - 33 percent had no plans to leverage security analytics

Supporting Quotes

â€œLoss of IP and competitive advantage, diminishing brand value, loss of customers and negative shareholder impact are just a few of the business impacts many organizations felt as a result of cyber-attacks this year,â€said Adam Bosnian, executive vice president, CyberArk. â€œThis yearâ€™s survey results demonstrate that whether itâ€™s an insider like Edward Snowden, or an outside-based attack like the retail/PoS breaches, attackers require the exploitation of insider credentials to successfully execute their attacks.â€

Full Research Brief:

http://www.cyberark.com/resource/global-advanced-threat-landscape-survey-2014

About CyberArk

CyberArk is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the worldâ€™s leading companies â€“ including more than 35 percent of the Fortune 100 and 17 of the worldâ€™s top 20 banks â€“ to protect their highest value information assets, infrastructure and applications. A global company, CyberArk is headquartered in Petach Tikvah, Israel, with U.S. headquarters located in Newton, MA. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com, read the company blog, http://www.cyberark.com/blog/, follow on Twitter @CyberArk or Facebook at https://www.facebook.com/CyberArk.