Global Survey: Cyber Attackers Posing as Legitimate Insiders Represent Greatest Security Risks

September 30, 2015 7:00 AM ET

61 Percent Cite Privileged Account Takeover as Most Difficult Cyber Attack Stage to Mitigate; 44 Percent Still Believe They Can Prevent Attackers from Breaking into a Network

NEWTON, Mass.--(BUSINESS WIRE)--Sep. 30, 2015-- Cyber attacks that exploit privileged and administrative accounts – the credentials used to manage and run an organization's IT infrastructure – represent the greatest enterprise security risks, according to a new survey released by CyberArk (NASDAQ: CYBR).

Sixty-one percent of respondents cited privileged account takeover as the most difficult stage of a cyber attack to mitigate, up from 44 percent last year. In addition, 48 percent believe that data breaches are caused by poor employee security habits, while 29 percent blame attacker sophistication. The findings are part of CyberArk's 9th Annual Global Advanced Threat Landscape Survey, developed through interviews with 673 IT security and C-level executives.

CyberArk analyzed potential discrepancies between damaging cyber security threats and organizations' confidence in being able to defend themselves. While there is increasing awareness about the connection between privileged account takeover as a primary attack vector and recent, high profile breaches, many organizations are still focusing on perimeter defenses.

With more than half of respondents believing they could detect an attack within days, CyberArk warns that many IT and business leaders may not have a full picture of their IT security programs. Looking beyond the tip of the iceberg with perimeter defenses and phishing attacks – organizations must be able to protect against more devastating compromises happening inside the network, like Pass-the-Hash and Kerberos 'Golden Ticket' attacks.

Key findings of the 2015 survey include:

Beyond the Breach – Attackers Going for Complete Network Takeover

As demonstrated by attacks on Sony Pictures, the U.S. Office of Personnel Management (OPM) and more, once attackers steal privileged accounts, they can conduct a hostile takeover of network infrastructure or steal massive amounts of sensitive data. These powerful accounts give attackers the same control as the most powerful IT users on any network. By being able to masquerade as a legitimate insider, attackers are able to continue to elevate privileges and move laterally throughout a network to exfiltrate valuable data.

- Respondents were asked which stage of an attack is the most difficult to mitigate:
  - 61 percent cited privileged account takeover; versus 44 percent in 2014
  - 21 percent cited malware installation
  - 12 percent cited the reconnaissance phase by the attackers
- Respondents were asked what attack vectors represented the greatest security concern:
  - 38 percent cited stolen privileged or administrative accounts
  - 27 percent cited phishing attacks
  - 23 percent cited malware on the network

False Confidence in Corporate Security Strategies

CyberArk's survey highlights that while respondents display public confidence in their CEOs' and directors' security strategies, the tactics being employed by organizations can contradict security best practices. Despite industry research showing that it typically takes organizations an average of 200 days to discover attackers on their networks, a majority of respondents believe they can detect attackers within days or hours. Respondents also persist in believing that they can keep attackers off the network entirely – despite repeated evidence to the contrary.

- 55 percent believe they can detect a breach within a matter of days; 25 percent believe they can detect a breach within hours
- 44 percent still believe that they can keep attackers off of a targeted network
- 48 percent believe poor employee security habits are to blame for data breaches; 29 percent believe attackers are simply too sophisticated
- 57 percent of respondents were confident in the security strategies set forth by their CEO or Board of Directors

Organizations Fail to Recognize Dangers of Attacks on the Inside

Cyber attackers continue to evolve tactics to target, steal and exploit privileged accounts – the keys to successfully gaining access to an organization's most sensitive and valuable data. While many organizations focus heavily on defending against perimeter attacks like phishing, attacks launched from inside an organization are potentially the most devastating. Respondents were asked to rank the type of attacks they were most concerned about:

- Password hijacking (72 percent)
- Phishing attacks (70 percent)
- SSH key hijacking (41 percent)
- Pass-the-Hash attacks (36 percent)
- Golden Ticket attacks (23 percent)
- Overpass-the-Hash attacks (18 percent)
- Silver Ticket attacks (12 percent)

Overpass-the-Hash, Silver Ticket and Golden Ticket are types of Kerberos attacks, which can enable complete control over a target's network by taking over the domain controller. One of the most dangerous is a Golden Ticket attack, which can mean "game over" for an organization and complete loss of trust in the IT infrastructure.

"It is no longer acceptable for organizations to presume they can keep attackers off their network," said John Worrall, CMO, CyberArk. "The most damaging attacks occur when privileged and administrative credentials are stolen, giving the attacker the same level of access as the internal people managing the systems. This puts an organization at the mercy of an attacker's motivation – be it financial, espionage or causing harm to the business. The survey points to increasing awareness of the devastating fallout of privileged account takeover, which we hope will continue to spur a ripple effect in the market as organizations acknowledge they must expand security strategies beyond trying to stop perimeter attacks like phishing."

Survey Results

Complete Global Advanced Threat Landscape Survey results can be downloaded for free at http://www.cyberark.com/ThreatSurvey2015.

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 world's leading companies – including 40 percent of the Fortune 100 and 17 of the world's top 20 banks – 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, Mass. 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.

Forward-Looking Statements

This release may contain forward-looking statements, which express the current beliefs and expectations of CyberArk's management. Such statements involve a number of known and unknown risks and uncertainties that could cause the Company's future results, performance or achievements to differ significantly from the results, performance or achievements expressed or implied by such forward-looking statements. Important factors that could cause or contribute to such differences include risks relating to: changes in the new and rapidly evolving cyber threat landscape; failure to effectively manage growth; fluctuations in quarterly results of operations; real or perceived shortcomings, defects or vulnerabilities in the Company's solution or the failure of the solution to meet customers' needs; the inability to acquire new customers or sell additional products and services to existing customers; competition from IT security vendors and other factors discussed under the heading "Risk Factors" in the Company's most recent annual report on Form 20-F filed with the Securities and Exchange Commission. Forward-looking statements in this release are made pursuant to the safe harbor provisions contained in the Private Securities Litigation Reform Act of 1995. These forward-looking statements are made only as of the date hereof, and the Company undertakes no obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise.

View source version on businesswire.com: http://www.businesswire.com/news/home/20150930005161/en/

Source: CyberArk

Media Relations Contacts:
fama PR
Brian Merrill, +1-617-986-5005
cyberark@famapr.com
or
CyberArk
Liz Campbell, +1-617-558-2191
press@cyberark.com
or
Investor Relations Contact:
ICR
Staci Mortenson, +1-617-558-2132
IR@cyberark.com