CyberArk Security Brief: Securing Third-Party Remote Access, a Weak Link in Enterprise IT

April 8, 2015 9:01 AM ET

Most Leading Institutions Have 200-300 High-Risk, Third-Party Relationships; CyberArk Provides Best Practices for Strengthening an Enterprise IT Weakness Exploited by Attackers

NEWTON, Mass.--(BUSINESS WIRE)--Apr. 8, 2015-- CyberArk Software Ltd. (NASDAQ: CYBR), the company that protects organizations from cyber attacks that have made their way inside the network perimeter, today released a new security brief to protect organizations against cyber attacks through third-party remote access points. The brief, "Securing Remote Vendor Access with Privileged Account Security," and accompanying Infographic can be downloaded for free: www.cyberark.com/remote-vendor.

"It's no secret that attackers target the weakest links in IT security, which are often found in accounts provisioned to third-parties for network access," said John Worrall, Chief Marketing Officer, CyberArk. "Often, these smaller third-party organizations have less sophisticated security policies and controls than the target companies, providing an open backdoor for attackers. With the proper privileged account security controls in place, organizations can provide the network access required for business efficiency while maintaining consistent security across all types of accounts – internal and external."

The Third-Party, Remote Access Problem

High-profile attacks reveal that malicious hackers target third-party vendors and supply chain partners as a backdoor into their primary target. Organizations in every industry provide network access to third-party vendors, which range from services companies and suppliers to external consultants.

Attackers target less secure partners to compromise remote access points, steal and exploit privileged credentials, and gain access to targeted networks. From here, attackers can elevate privileges, move laterally through the network, and execute their attack goals while completely circumventing the targeted company's defenses.

According to recent research[i], attackers are increasingly targeting this soft spot in cyber security:

- 60 percent of organizations allow third-party vendors remote access to internal networks[1]
  - Top U.S. banks and credit companies average nearly 20,000 third-party suppliers[2]
  - Most leading institutions have 200-300 high-risk, third-party relationships[2]
  - Third-party errors increase the cost of a data breach by as much as $43 per record in the U.S.[3]
- 100 percent of advanced attacks exploit privileged credentials[4]
- 63 percent of data breaches are caused by security vulnerabilities introduced by third parties[5]
- 58 percent of organizations have no confidence that their third-party vendors are securing and monitoring privileged access to their network[1]

The CyberArk security brief provides organizations with guidance on how to address remote vendor access as a privileged access point that requires tight security controls. Topics covered include: approaches for managing and securing third-party credentials, how to isolate and monitor external sessions, and the importance of threat detection capabilities in security solutions for third-party access.

To download and use the CyberArk Infographic "Third-Party Access: The Hidden Weak Spot Exploited by Attackers," please visit: www.cyberark.com/remote-vendor-infographic.

To download a free copy of CyberArk's security brief on securing remote vendor access, please visit: www.cyberark.com/remote-vendor.

About CyberArk
CyberArk (NASDAQ: CYBR) 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, MA. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com.

Cautionary Language Concerning 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 annual report on Form 20-F filed with the Securities and Exchange Commission on February 27, 2015. 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.

[i] Sources:

[1]CyberArk 8th Annual Global Advanced Threat Landscape Survey, 2014

[2]McKinsey & Company: Managing Third-Party Risk in a Changing Regulatory Environment, May 2013

[3]Ponemon Institute 2013 Cost of Data Breach Study: Global Analysis

[4]CyberSheath, "APT Privileged Account Exploitation," April 2013

[5]Computerworld: Hackers Hit More Businesses Through Remote Access Accounts, July 2, 2014

Photos/Multimedia Gallery Available: http://www.businesswire.com/multimedia/home/20150408005239/en/

Source: CyberArk Software Ltd.

Media Relations Contacts:
fama PR
Brian Merrill, +1-617-986-5005
cyberark@famapr.com
or
CyberArk
Christy Lynch, +1-617-796-3210
press@cyberark.com