NorthJersey.com

APRIL 15, 2014, 9:00 AM
LAST UPDATED: TUESDAY, APRIL 15, 2014, 9:21 AM

North Jersey tech companies react to Heartbleed bug

BY ANDREW WYRICH
STAFF WRITER | THE RECORD

North Jersey technology companies are reacting to last week's announcement that a flaw in the widely used software OpenSSL could have affected as many as 500,000 popular websites and exposed millions of Internet users to possible breaches in their security.

The programming error nicknamed "Heartbleed" is a weakness found in the OpenSSL software that could expose website users to hackers looking to steal passwords or other sensitive information. OpenSSL is a free encryption software meant to provide secure communications and is used by as many as 66 percent of all active Internet websites, according to a survey by Internet services website Netcraft.com. OpenSSL works with a Web user by utilizing encrypted "keys" to send information back and forth, such as when a user enters a password for an email account.

The common logo used to depict the Heartbleed bug.

The Heartbleed bug, announced last week by researchers from Google and a Finland-based company, Codenomicon, may have let hackers silently extract data from a computer's memory for years before its discovery was made public. The bug could allow third parties to have access to the encryption used for communicating information such as passwords to websites. For two years any app, website or private messaging app that used the vulnerable OpenSSL had been open to hacking.

Popular websites such as Yahoo, Tumblr, OKCupid and Pinterest were among sites at risk, according to the tech website Mashable.com. Email providers such as Yahoo Mail and Gmail also were vulnerable to the bug, according to the website.

Because attacks would not leave traces on server logs, it is still unknown if cybercriminals or state-sponsored hackers used Heartbleed to steal private information over the two years this vulnerability was present.

A patch for Heartbleed was released April 7, and several North Jersey companies have begun working with customers to ensure their products have been updated and are secure.

Radware Inc., a Mahwah-based Internet security firm, said Monday it has updated some of its software for free to help customers such as Papa John's Pizza, Ace Hardware, game company Konami and Hewlett-Packard receive protection from Heartbleed.

While most of the security products offered by the company were not subjected to the Heartbleed bug, two specific versions of its products required an update, according to Radware's website.

The company said in response to the Heartbleed fallout that it has updated its Internet-defense product DefensePro. That product will detect potential Heartbleed exposure and will continue to monitor the situation to see if more protections will be needed in the future.

"As the Heartbleed bug affects many businesses, we wanted to help navigate our customers through this, as well as others who may have been looking for solutions to help them mitigate this threat," Brian Gallagher, a spokesman for Radware, said. "As the full scope and magnitude is yet to be fully determined, this is a serious vulnerability that we treated with the utmost importance."

Other North Jersey tech companies are also addressing the Heartbleed issue.

Clifton-based Comodo Group Inc. is the second-largest company in terms of issuing "digital certificates" that encrypt traffic between users of a website and the Web service itself, shielding users from third parties such as hackers.

In an interview with PCWorld.com last Friday, Comodo Chief Technology Officer Robin Alden said the company has seen a surge in the amount of requests from website operators to receive new digital certificates since the revelation of Heartbleed.

"The last couple of days, we've seen replacement rates running at somewhere between 10 to 12 times the normal rate," Alden told PCWorld. "That's obviously fallout from this."

Alden is in the United Kingdom this week and was not available for comment.

Comodo has contacted customers and conducted automated scanning to find websites using its certificates that could have been vulnerable to Heartbleed, according to the article.

Email: wyrich@northjersey.com Twitter: @AndrewWyrich