Heartbleed - Risk In The Shadows

by Steve Brown

If you turn on the news at any point during the day, you are likely to see commercials about various maladies that you never knew existed. These ills can be cured with prescription medication, but it all seems to have spooky side effects. Now there is a new malady on the cyber risk front called "Heartbleed." This new cyber disease is apparently already 2Ys old and may have been stealing your information since then. For banks and customers of banks, this vulnerability is causing much more than a headache.

To start, Heartbleed is a hole in software security that allows ne'er-do-well's to steal protected information, like passwords. The bad guys can eavesdrop on communications, steal data and even impersonate users and services. This vulnerability was found in the OpenSSL cryptographic software library, which is only important because it is estimated to encrypt web communication on around 66% of all active sites worldwide.

As everyone knows who has had a computer problem in the past, it is a royal pain but it is not usually life-changing. This vulnerability may prove to be different however so taking action makes sense. Basically, this vulnerability may open up the security of your system and leaves personal information open to a third-party attack. Not only does this vulnerability exist on many sites, it can also affect internal systems that are web-enabled.

This could mean that despite all your hard work to get creative with your password combinations, even the most diligent and security conscious of us must assume many passwords may have already been exposed.

To protect yourself, experts suggest quickly changing passwords for the web sites you use. These should include email, social media, bank accounts, credit card online access and others. To find out whether the sites you commonly use are affected you can visit sites like mashable to see a list: http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/.

As for our own testing, we decided to call a couple of big credit card companies to see whether their sites were fixed before we changed our passwords. Our questions were met with puzzlement by some operators (who were not aware of the issue), while others referred us to their security protocols. The entire process was not reassuring, so we recommend bankers get patches loaded, alert staff to the problem and be sure everyone can speak intelligently to concerned customers.

For their part, bank regulators are also warning institutions to "actively utilize available resources to identify and help mitigate potential cyber-related risks." They want all banks to "be aware of the constantly emerging cyber threats and government-sponsored resources available to help identify these threats on a real-time basis." For bankers, resources highlighted include: the United States Computer Emergency Readiness Team; Secret Service Electronic Crimes Task Force; FBI InfraGard; Regional Coalitions and Information Sharing and Analysis Centers.

If there is any good news in all of this it is the fact that while alarming, at least we now all know our passwords may be compromised. Maybe it is time to change them anyway and to be sure, not every

site that uses Open SSL is at risk (many use additional encryption software so probably aren't vulnerable).

As we close off today, we remind our readers that this vulnerability is due to a hole in software security that allows hackers to read the memory of systems protected by vulnerable versions of OpenSSL software. While that includes lots of known companies, patches are flying out and many have already taken steps to fix this issue.

As for PCBB - we have multiple layers of security to protect our customers and use encryption that is not known to be vulnerable to Heartbleed. Your customers will probably also want to know your bank is safe, so let them know as soon as you can. Unfortunately given the depth of this vulnerability, this looks like it that will take time to cure and likely have odd side effects that show up over time.

BANK NEWS

Branch Sale

Talmer Bank ($2.3B, MI) will sell 11 branches in WI to Wintrust Financial ($18.1B, IL) for $13.5mm more than net book value according to financial filings. The branches hold about $360mm in deposits.

Competition

Bank of America Merrill Lynch has added bill pay to its suite of payments solutions for business clients. The product, called CashPro BillPay, allows business customers to control the timing of payments to better manage cash flows. CashPro integrates into most accounting packages, provides a document repository, eliminates the need for check printing, mailing and storage and automatically links to vendors that accept electronic payments.

Settlement

Citigroup will pay $1.1B to settle claims with 18 institutional investors related to $59B of private label residential securities it issued from 2005 to 2008.

Huge Fine

Bank of America will pay $772mm ($45mm fine and $727mm in restitution to affected consumers) to settle OCC and CFPB allegations it engaged in unfair fee collection and marketing related to credit card add-on products. The regulatory agencies said marketing these products as identity theft protection violated laws.

Large Layoffs

Bank of America said it will lay off 3,000 employees and close three overseas offices that handle technology and operations.