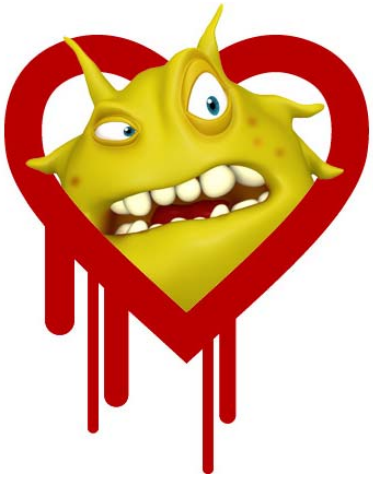
Issue # 4 Volume #15 April 2014

Solutions are our Business

Heartbleed

Last week, a new bug took the Internet by storm. Causing panic and uncertainty, Heartbleed managed to rock the core of the Internet world. Heartbleed is not a virus but is a major vulnerability which is found in OpenSSL cryptographic software. It has the potential to uncover user names, passwords and credit card information, allowing attackers to view the actual content and/or infiltrate website services by using the private SSL key. This type of information under normal circumstances, is protected by the SSL/TLS encryption used to secure the Internet.

SSL/TLS provides security over the internet for emails, Instant Messaging, two-thirds of all websites, and some virtual private networks (VPN). What was also discovered last week was that the bug not only affected websites, it also penetrated through routers, servers, video games and mobile phones. According to CNN money, Heartbleed is being named the biggest exploit in the past twelve years. This security flaw has made it very easy for hackers to steal personal information and go virtually undetected. The bug is extremely serious and is believed to have affected over 500,000 websites.



While there is lots of information buzzing around the Internet, the good news is most sites that were affected by the bug most likely have already patched the risk. Despite this, here are some basic guidelines that can help you and your customers be more secure when it comes to Internet security.

⇒ Change your passwords - To be on the safe side, we recommend all passwords for all your online accounts be changed once you get confirmation that the site is not or is no longer vulnerable.

⇒ Enable dual-factor authentication when it is offered - That means that in addition to a password, the service asks for another piece of identifying information, like a code that's been texted to you.

⇒ Check the status of the websites that you visit by going to http://filippo.io/Heartbleed/. This website was created specifically to help the public determine which websites have been affected by Heartbleed.

⇒ Let AaSys and Focus Audits assist -Focus Audits can provide external and internal scanning specifically to identify the Heartbleed vulnerability. The scanning can be completed for your outside facing IP addresses as well as your internal IP addresses. Contact your Account Executive for more information.

AaSys has taken all the necessary steps to ensure our customers are protected and that your information is safe. We are staying on top of this situation and if any additional information becomes available we will be sure to reach out to you.

Are there subjects that you would like to have covered in future newsletters? We are always looking for topics of interest and we welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please send an email to newsletter@aasysgroup.com

11301 N. US Highway 301, Suite 106
Thonotosassa, FL 33592
(800) 799-8699
www.aasysgroup.com

Inside this issue:

Alert: ATM Cyber Attack

> "A recent Unlimited Operations attack netted over $40 million in fraud using only 12 debit card accounts."

It has been a busy year for cyber criminals and it is clear they are not letting up. Early this month Federal Regulators put financial institutions on notice about an ATM cyber-attack which used twelve debit cards to withdraw over forty million dollars out of ATM machines. The Secret Service is calling this attack "Unlimited Operations."

This attack allowed the criminals to withdraw funds beyond the cash availability of the account. The attacks generally come through phishing emails to employees of financial institutions. Once the malware penetrates the financial institution's network, the attackers then are able to monitor how the organization accesses money through the ATM control panels. The control panels monitor how much can be withdrawn from an account at any given time.

The attackers obtain employee log in credentials allowing them to change the control panel's settings, permitting debit cards they previously stole to withdraw unlimited amount of funds.

Federal Regulators along with the FDIC are advising that any institution which issues debit cards, credit cards or pre-paid cards be very vigilant with their security.

They are also urging community banks with ATMs to work closely with their service providers to ensure the providers are taking appropriate action to mitigate this risk.

Here are some of the steps that Federal Regulators recommend financial institutions take:

⇒ **Conduct ongoing information security risk assessments**

⇒ **Perform security monitoring, prevention, and risk mitigation**

⇒ **Protect against unauthorized access**

⇒ **Implement and test controls around critical systems regularly**

⇒ **Conduct information security awareness and training programs**

⇒ **Test incident response plans**

SPECIAL ANNOUNCEMENTS

Save the Date

Back by popular demand, AaSys Group is pleased to present the next **Florida ISO Peer Group Meeting.**

We will be discussing the very critical and timely topic of ***Framework for Improving Critical Infrastructure Cybersecurity***. The open discussion at the end of the meeting will allow you to ask questions and share your experiences with your peers. This is also a great opportunity to network with others throughout the state to discuss some of the most critical issues facing the financial services industry today.

The meeting will be on June 19, 2014 between 10:00 am and 2:00 pm. More details on the location will be provided soon, although the Central Florida area seems to be the most conveniently located for the past attendees.

Happy Easter!

Did you know…

- After Halloween, Easter is the biggest candy consuming holiday. 120 million pounds of candy are bought each year, enough to fill four dump trucks.
- Households spend $131 on Easter each year, $14.7 billion in total.
- 90 million chocolate bunnies, 91.4 billion eggs and 700 million peeps are produced each year in the United States.
- 76% of people eat the ears on chocolate bunnies first.
- Americans consume over 16 million jellybeans on Easter, enough to