Issue # 5 Volume #15 May 2014

Solutions are our Business

Internet Explorer Glitch

We just recently dealt with what potentially could've been a devastating security issue with the Heartbleed vulnerability, and then we are hit with another blow. Microsoft announced on April 27th , that there was a huge security flaw in Internet Explorer versions 6 to 11. The "Microsoft Internet Explorer Remote Code Execution Vulnerability" affected all Internet Explorer versions using Adobe Flash. The bug allowed hackers the same amount of access on the network as a legitimate user and let hackers gain access to user's personal information.

The people most at risk were those still using Windows XP operating system. Hackers have already used the vulnerability to launch limited attacks. This exploit was triggered on a system which accessed a malicious site using Internet Explorer or any of the components thereof. Programs such as Outlook, Outlook Express, and Windows Mail opened HTML email messages via IE controls, but the good news was that they did so in a "restricted sites" zone which helped protect the operating system. However, clicking a link to access a site via Internet Explorer could have still triggered the bug.

The Department of Homeland Security issued an advisory asking everyone NOT to use Internet Explorer until the bug had been fixed. Fortunately, Microsoft was able to deliver a patch on May 1, 2014 to fix the problem. They also delivered the patch not only for current versions of Internet Explorer, but also for users of Windows XP operating system, despite discontinuing technical assistance and updates for the 12-year-old operating system last month. One blog post said, ""The threat landscape has changed, and attackers have become more sophisticated."

AaSys understands that internet security is vital for our customers. On Monday April 28 we issued an alert via our Portal system (https://portal.aasysgroup.com) to all ROC customers. We began compatibility testing of a script to disable this vulnerability in Internet Explorer.

On Tuesday April 29th, we received word from Fortinet, Cisco and other firewall vendors that they had released an IPS signature to block this vulnerability. As a result, AaSys delayed the roll out of the script we had been testing. On May 1st, Microsoft released patch MS14-012 to address the vulnerability. AaSys sent out an email security advisory and began to roll out the patch immediately to all ROC customers.

As always, AaSys will continue to be diligent in making sure YOU are as protected as can be. We will continue to be vigilant with internet security and will keep all our customers abreast of any issues that may arise.

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

AaSys will be closed on Monday, May 26th in observance of Memorial Day.

Inside this issue:

CLICK PROTECT

For many of us, our email is our lifeline. Sometimes it is the easiest and fastest form of communication. These days, we not only email each other for business, but we also send cards, invites, games, pictures, articles,…the list is endless.

Being able to be connected at anywhere anytime is just part of our culture and it is not changing. But being able to decipher what is a safe email or safe link in an email is even more crucial. Like we have discussed in the past, technology has its perks, but with that comes security concerns, especially with email.

Did you know that 95% of network attacks are a result of successful phishing attacks? And did you know that 79% of social breaches in 2012 were email based attacks? Wouldn't your mind be at ease knowing that emails you receive are being scanned for malicious malwares and viruses? McAfee Email Security offers a free feature called Click Protect. It is a complete email filtering system that protects against the latest threats, defeats zero-hour attacks, blocks phishing, advanced malware, and over 99% of spam well before they reach your network.

McAfee understands that better email security is needed to protect users against delayed malware attacks and wants to stop these attacks before they happen. If you want to know more about McAfee Click Protect, contact your Account Manager. But in the meantime, test your skills. See how much you really know about phishing attacks by taking this quiz on MacAfee's website. The results may surprise you! https://hishingquiz.mcafee.com/

Some of the Most Common Mistakes in Email Security

Not closing the browser after logging out.
When you are checking your email at a library or cybercafé you not only need to log out of your email when you are done, but you also need to make sure to close the browser window completely.

Forgetting to delete browser cache, history and passwords.
After using a public terminal, it is important that you remember to delete the browser cache, history, and passwords. Most browsers automatically keep track of all the web pages that you have visited, and some keep track of any passwords and personal information that you enter in order to help you fill out similar forms in the future.

Using unsecure email accounts to send and receive sensitive corporate information.
Careless employees sometimes use personal email accounts to conduct company business and pass along sensitive data that can undermine the security measures in place.

Solutions

SPECIAL ANNOUNCEMENTS

Save the Date

For the first time ever AaSys is offering the ISO Peer Group Meeting in Tennessee! On June 12th, in Sevierville, TN, AaSys will gather with bankers in that community to discuss the ***"The Overall Responsibilities and Challenges of an ISO Officer".*** The group will also be joined by FBI Special Agents who will discuss the latest trends in cyber attacks.

The meeting will start at 11 am and will be held at Hampton Inn & Suites, 105 Stadium Drive, Sevierville, TN (at Exit 407 off I-40). ***Don't miss it!***

Also in June, AaSys will hold the **Florida ISO Peer Group Meeting in Lake Mary, FL.**

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 attendees to ask questions and share personal experiences with 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 19th, between 10 am and 2 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.

Be sure to mark your calendars! We look forward to seeing you there!

We honor those who have fought and continue to fight for our freedom at home and overseas. We are forever indebted to our soldiers for giving the ultimate sacrifice for our country.

Happy Memorial Day!