Issue # 11 Volume #15 November 2014

AaSys® Solutions

Solutions are our Business

Domain Hijacking

Over the weekend, many who tried to log on to the popular Craigslist.com site got a bit of an odd response and were redirected to another site called DigitalGangster.com. What happened? What most big online companies fear the most: their domain name had been hijacked. Of course, this caused a major headache for Craigslist and its users, and one can only imagine the financial damage that may have resulted because of it. Thankfully, as of Monday morning the issue has been fixed but it still leaves many feeling uncertain. This clearly shows that no company is too big or too small to fall victim to this kind of attack. The key is to avoid becoming a victim in the first place.

Monitoring your Domain Name System (DNS) Traffic—it is very important to have a system in place that sends alerts when unusual DNS activity is detected. If your network does come under a Distributed Denial of Service (DDoS) attack, being alerted immediately allows you to quickly work with your providers to have the malicious traffic blocked.

You should also have a strong Password—making your password "bulletproof" is key. A pass-

word should be long and diverse enough to withstand any attempts by hackers to unlock. Also, you should use providers who offer multi-factor authentication and who have lock-out systems in place to prevent script attacks. DNS administrators should never use an e-mail address provided by a third-party webmail service such as Hotmail or GMail for their important, corporate login and contact details. These types of service are under constant attack. If an attacker can take over a webmail account used in managing DNS, the domains themselves are compromised as well.

Attackers typically use a phishing method or other social engineering tricks to gain access to online accounts that control the domain name services. However, attacks like these are usually simple to deal with and most of the time do not affect customers' data.

In conclusion, your domain name serves as a lifeline for your online existence and should be protected as such. Making sure your organization has good security practices in place may help eliminate a successful attack.

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

REMINDER!
The AaSys Help Desk will be closing at 5:00PM EST on November 28, 2014 and 4:00PM EST on December 24, 2014.

AaSys wishes you and your family a very Happy Thanksgiving!

Inside this issue:

Back By Popular Demand!!

Back by popular demand, AaSys Group is happy to announce another round of ISO Peer Group Meetings in Alabama and Tennessee!

In Alabama we will be discussing Vendor Management, Cybersecurity and Business Continuity Plans. In Tennessee, the agenda includes the NIST Framework for Improving Critical Infrastructure Cybersecurity. The open discussions 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. Be sure to mark your calendars! Check out the details below and we look forward to seeing you there!

Calera, Alabama

Date: December 9, 2014

Time: 10:30AM –2PM EST

Cohosted by Central State Bank

Location: Calera Community Center
8560 Highway 31
Calera, AL 35040

Topics: Vendor Management, Cybersecurity, Business Continuity Plans

Troy, Alabama

Date: December 11, 2014

Time:10:30AM –2PM EST

Cohosted by Troy Bank & Trust

Location: Troy Bank & Trust
1429 US 231 S
Troy, AL 36081

Topics: Vendor Management, Cybersecurity, Business Continuity Plans

Sevierville, TN

Date: December 09, 2014

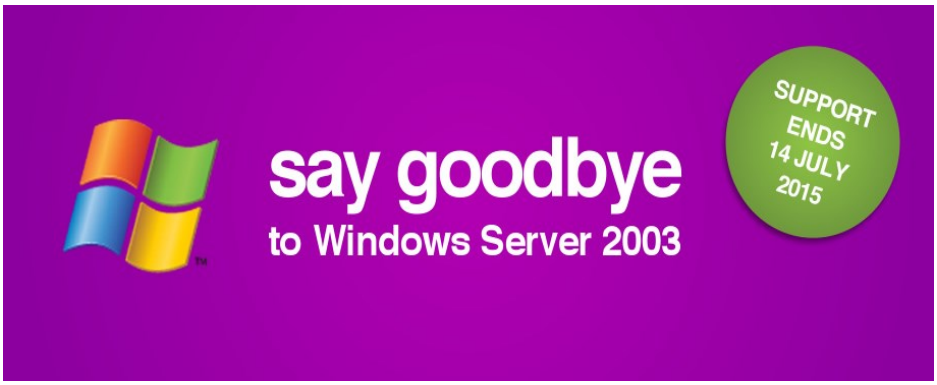
Time: 10:30AM –2PM EST

Location: Hampton Inn & Suites, 105 Stadium Drive, Sevierville, TN (at Exit 407 off I-40)

Topic: NIST Framework for Improving Critical Infrastructure Cybersecurity

Microsoft Ending Support for Windows Server 2003

The count down is on! On July 14, 2015, Microsoft will be ending support for Windows Server 2003. This means that those still using that operating system will no longer receive crucial security patches that help protect against viruses, spyware and malicious software. Users may also encounter problems with software and hardware compatibility since new software applications and hardware devices may not be built for Windows Server 2003. Computers using the old software will still work however, the risk of viruses and other malicious attacks increases exponentially and could result in significant loss of data, business assets, and confidential documents.



Don't wait until the last minute to make changes. July 14, 2015 will be here sooner than you think! AaSys can help you every step of the way. To see how we can assist in making this a smooth transition for your organization, please contact your Account Manager today!