Michigan Cyber Initiative News

March 2013, Issue 13

Articles of Interest

President Obama Issues Executive Cybersecurity Order
This new Executive Order focuses on improving cybersecurity for critical Infrastructure by creating a framework to reduce cyber risk and identifying critical infrastructure that is at the greatest risk. — Read this article here.

Banking Malware Returns to Basics to Evade Detection, Trusteer Says
Malware authors add phishing-like credential theft capabilities to banking Trojan programs, researchers from Trusteer say. — Read this article here.

Beware! Identity Thieves are Targeting Your Tax Refund
Tax identity theft is costing the government billions of dollars and entangling taxpayers in untold administrative hassle. — Read this article here.

Facebook Defends Graph Search's Privacy Controls for Teens
The site explains how search results for minors are displayed with its new search tool. — Read this article here.

350,000 Different Types of Spam SMS Messages were Targeted at Mobile Users in 2012
The most common spam messages claim to offer gift cards or iPhone and iPad giveaways. — Read this article here.

Did You Know?

The final rule for changes to the Health Insurance Portability and Accountability Act (HIPAA) has been announced.

A quick overview of some of the changes include:

- Increased penalties
- A more objective breach notification standard
- An expanded business associate definition.

The final rule will become effective March 26, 2013, and the compliance deadline is Sept. 23, 2013.

More details on the changes and the source of this information can be found at Thompson Coburn LLP. You can also visit the U.S. Department of Health and Human Services to view the press release and final rule.

The Survey Results Are In!

Thank you to the attendees of the breakfast series and the participants of the survey. We received a lot of positive feedback and suggestions that will be considered while planning this October's Cyber Summit.

From the results, 100% of those surveyed found the breakfast series beneficial and that it met their expectations.

One individual asked that we provide updates on how Michigan is advancing as a state via the Governor's strategy to be a leader in cybersecurity. Those updates can be found in this newsletter as we continue to work on Governor Snyder's Cyber Initiative.

Our accomplishments so far include the opening of the Cyber Range, which has received national attention and will have classes available starting this spring. Find out more here.

In addition, we have rolled out cybersecurity awareness training to State of Michigan employees. You can read more about this in an article found here.

Passing PCI Compliance Scans in the Public Cloud

To protect highly sensitive cardholder data, the Payment Card Industry Security Standard Council (PCI SSC) released 12 Top Level Data Security Standards (DSS). Financial organizations are required to validate their adherence to certain DSS requirements. Below is an overview of the 12 PCI DSS requirements.

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**Requirement 3:** Protect stored cardholder data **Requirement 4:** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**Requirement 5:** Use and regularly update anti-virus software **Requirement 6:** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**Requirement 7:** Restrict access to cardholder data by business need-to-know **Requirement 8:** Assign a unique ID to each person with computer access **Requirement 9:** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**Requirement 10:** Track and monitor all access to network resources and cardholder data **Requirement 11:** Regularly test security systems and processes
Maintain an Information Security Policy	**Requirement 12:** Maintain a policy that addresses information security

There are more than 130 Approved Scanning Vendors (ASVs) that can be used to detect vulnerabilities found in a public cloud. CloudAccess.net, a Michigan-based Platform as a Service (PaaS), used McAfee and Comodo to perform security scans on targeted hosting environments. Using the results, the company adjusted server specifications to pass subsequent scans, ultimately helping several clients validate the security of their content including Reliance Bank, a full service bank with 20 branches in the St. Louis metropolitan region, and CIMA (the Center for Information Management and Assurance), an organization that aims to elevate the information security community. CloudAccess.net is helping clients pass ASV scans on an individual basis, but the company is developing an automated PCI-DSS hosting layer that can be applied to any environment with a click of a mouse.

Passing an ASV scan is a critical part of the PCI testing system, but it is very important to note that passing such scans doesn't necessarily mean that the hosting environment reaches the highest levels of PCI-DSS standards. To learn more, visit pcisecuritystandards.org and read about Navigating PCI DSS.

Author: Ryan Bernstein is the Chief Operating Officer, Technical Writer and Content Manager for CloudAccess.net and a professor in the communications department at Northwestern Michigan College in Traverse City, Michigan.

European Report Says Cyber Attacks Target Trust

The European Network and Information Security Agency (ENISA), which is a part of the European Union (EU), recently issued a report that describes the current global cyber threat landscape. The excellent report "is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends."

Excerpted by permission from Lohrmann on Cybersecurity, www.govtech.com, Jan. 14, 2013.