Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

April 6, 2015

Eight (8) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

MidAtlantic Collegiate Cyber Defense Competition: Results

The Mid-Atlantic Collegiate Cyber Defense Competition (www.maccdc.org) was a great success! On March 26-28, 2015, 10 university and community college teams who advanced from virtual qualifiers earlier in the month battled it out at the Kossiakoff Center at JHU's Advanced Physics Lab for the privilege of representing the Mid Atlantic region in the national Collegiate Cyber Defense competition. The results were an all-Maryland sweep:

1. Univ. of MD Baltimore County
2. Univ. of MD College Park
3. Towson

The national competition will take place in San Antonio TX from April 24-26, 2015 (http://www.nationalccdc.org/)

Cyber Security Policy News

Events

See Upcoming Events at a Glance

Click here for detailed descriptions

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

Sanctions for cyberattacks

-Declaring cyberattacks a "national emergency," President Obama last week issued an executive order that would allow the United States to inflict financial penalties on those thought to be behind the attacks. The order allows the secretary of the Treasury, in consultation with the attorney general and secretary of State, to impose financial sanctions-such as freezing of assets or prohibition of commercial trade-on individuals or groups responsible for malicious cyberattacks that "create a significant threat to U.S. national security, foreign policy, or economic health or financial stability of the United States," writes Dustin Volz of National Journal. "Administration officials have long indicated a desire to strengthen the government's ability to respond to and penalize those engaging in cyberattacks. The massive hit on Sony Pictures last Thanksgiving-which the White House publicly blamed on North Korea-increased the urgency to bolster the nation's cyber defenses. In January, Obama signed a separate executive order allowing for further sanctions against North Korean targets, but that action was limited to just that country."

But some experts say the new executive order raises questions about due process for people who feel they're wrongly accused and about how agencies will identify the source of attacks. Grant Gross of Computerworld writes that "attributing the source of cyberattacks is still difficult, and it's unclear what standard of proof the U.S. government will use to impose the new sanctions," Gross wrote. "In addition, the White House offered few details about how accused organizations can challenge the sanctions."

Many apparently state-sponsored cyberattacks that might trigger such sanctions go unreported by companies, according to a new report by Citigroup. The report warned that law firms are a major target of these attacks, because they hold so much valuable information about large companies. "The report said bank employees should be mindful that digital security at many law firms, despite improvements, generally remains below the standards for other industries," The New York Times reports. "It said law firms were at 'high risk for cyber intrusions' and would 'continue to be targeted by malicious actors looking to steal information on highly sensitive matters such as mergers and acquisitions and patent applications.'"

US military in need for cybersecurity talent

For its part, the U.S. military is so stretched for cybersecurity talent that it's willing to relax some of its enlistment standards, particularly for high-tech or cybersecurity jobs, according to the Associated Press. "Speaking to students at his former suburban Philadelphia high school, [Defense Secretary Ash] Carter said the military could ease age requirements and bring in older people who are mid-career, or provide student loan repayments to attract students who have finished college," writes Lolita C. Baldor. "There are few details so far, but Carter said the military needs to be more flexible in order to recruit and retain quality people. The idea, largely in line with the civilian approach to recruitment, upends the military's more rigid mindset, which puts a high value on certain standards. It reignites a persistent debate about how the services approve waivers for recruits who have committed lesser crimes, behaved badly, are older than current regulations allow or have other physical issues that prevent them from joining the military."

License plate dispute
-The dispute over whether government and state law enforcement and investigative agencies should be able to use license plate-reader is heading up. The Washington Post reports that the Department of Homeland Security is seeking bids from companies able to provide law enforcement officials with access to a national license-plate tracking system - a year after canceling a similar solicitation over privacy issues. "The reversal comes after officials said they had determined they could address concerns raised by civil liberties advocates and lawmakers about the prospect of the department's gaining widespread access, without warrants, to a system that holds billions of records that reveal drivers' whereabouts," according to Ellen Nakashima.

In Virginia, Gov. Terry McAuliffe (D) recently amended a significant license plate reader data retention bill, sending it back to state lawmakers, despite near-unanimous support in both houses of the Virginia state legislature. Ars Technicareports that had the bill passed, it would have imposed a limit of just seven days on keeping such data absent an ongoing criminal investigation.

About this Newsletter

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613. cspri@gwu.edu
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052