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

New!

Read more about CSPRI's education, research, and service projects with our new, interactive project wheel.

Click here.

April 27, 2015

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

Legislative Lowdown

-The House of Representatives last week easily passed cybersecurity legislation, despite increasingly vocal calls from privacy and civil liberties advocates to revamp the bill. "On Wednesday the House of Representatives voted 307-116 to pass the Protecting Cyber Networks Act, a bill designed to allow more fluid sharing of cybersecurity threat data between corporations and government agencies,"writes Andy Greenberg for Wired.com. "That new system for sharing information is designed to act as a real-time immune system against hacker attacks, allowing companies to warn one another via government intermediaries about the tools and techniques of advanced hackers. But privacy critics say it also threatens to open up a new backchannel for surveillance of American citizens, in some cases granting the same companies legal immunity to share their users' private data with government agencies that include the NSA."

-Lawmakers in the House and Senate have introduced measures that would exempt responsible hacking from prosecution under existing copyright law. "The security and academic community has long worried they could

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

face legal action for basic research, which often involves examining computer networks in a way that may technically run afoul of the Digital Millennium Copyright Act (DMCA)," writesCory Bennett for The Hill. "The DMCA forbids anyone from circumventing technological protections on copyrighted works." Backers of the bill charge that these provisions in the DMCA have had a chilling effect on research, and could prevent researchers from coming forward about fixing dangerous security vulnerabilities.

Congress also is considering another new bill aimed at helping security researchers, or at least not unduly punishing them with criminal charges. As the National Journal reports, more than two years after the death of Aaron Swartz, a programmer and online activist who took his own life after being charged with data theft, lawmakers are trying for a second time to pass a bill that would soften the terms of the law he was charged under. "Democratic Sen. Ron Wyden of Oregon and Democratic Rep. Zoe Lofgren of California on Tuesday reintroduced the so-called 'Aaron's Law,' which they say would clear up vague language in the Computer Fraud and Abuse Act to keep low-level violators from getting in trouble with the law," writes Kaveh Waddell for the Journal. Read more here.

Cyber Security Policy News

The President's Surveillance Program
-The government's efforts to collect information about Americans' calls and emails received mixed reviews from government officials, a once-classified report released last week reveals. "The redacted, six-year-old report, releasedSaturday by the Office of the Director of National Intelligence in response to a New York Times lawsuit, provides a detailed analysis of the 'President's Surveillance Program,' in which the government secretly collected communications information from Americans," writes Peter Schroeder for The Hill. "That program was revealed by Edward Snowden, a former National Security Agency contractor. According to the Associated Press, the review said some senior intelligence officials found worth in the program, saying it helped fill gaps in existing surveillance. But there were other federal agents and analysts that had difficulty measuring the 'precise contribution' of it, describing it as just 'one source among many.'"

Russian hackers breach the White House's unclassified system
-Some of President Obama's email correspondence was swept up by Russian hackers last year in a breach of the White House's unclassified computer system that was far more

intrusive and worrisome than has been publicly acknowledged, The New York Times reports. "The hackers, who also got deeply into the State Department's unclassified system, do not appear to have penetrated closely guarded servers that control the message traffic from Mr. Obama's BlackBerry, which he or an aide carries constantly," the Times wrote.

DoD unveils updated cybersecurity strategy
-The Department of Defense has unveiled an updated cybersecurity strategy that officially acknowledges for the first time that the U.S. military is willing to use cyberwarfare to defend U.S. interests against cyber-enemies, GovInfoSecurity reports. "In defending the country, 'if directed by the president or the secretary of defense, the U.S. military may conduct cyber operations to counter an imminent or ongoing attack against the U.S. homeland or U.S. interests in cyberspace,' the strategy states, according to Marianne Kolbasuk McGee. "The purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life."

Still using Windows XP
Japanese regulators told the company that operates the stricken Fukushima Daiichi nuclear energy complex to migrate 48,000 internet-connected PCs off Windows XP sooner rather than later, The Register reports. While there is no suggestion that the problems with The Tokyo Electric Power Company's reactor in the wake of the 2011 tsunami in Japan were at all connected to computer failures, Microsoft stopped supporting Windows XP last year, leaving the systems dangerously exposed to new-found security bugs.

U.S. Army wants to continue to use Windows XP
Meanwhile, the U.S. Army says it's seeking options for supporting some 8,000 Windows XP systems through April 2016. "After Microsoft ended software updates for the popular operating system in April 2014, the company offered "custom support" for $200 per device for the first year," writes Government Computer News. "After that first year, the cost of custom support was expected to double. Now the Army wants to find a company that will provide 100 percent of continued coverage for security updates for vulnerabilities rated "critical" and for security hotfixes rated "important" from May 1, 2015, through April 30, 2016, while the Army continues its migration off the outdated operating system."

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