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

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

June 15, 2015

Nine (9) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

-The House of Representatives last week passed a funding bill that would restrict government surveillance programs. Federal Computer Week writes: "Taken together, they constitute something of a follow-on to the USA Freedom Act, just signed into law, which put new rules on the bulk collection and searching of telephone metadata by spy agencies." Read onfor what the bill entails.

According to The Hill, the bill tackles two separate "backdoors" into people's communications about which lawmakers on both sides of the aisle have raised alarms. "One provision of the amendment would ban the government from forcing tech companies to build weaknesses into their security systems so that police and federal agents can access people's data,"writes Julian Hattem. "While the FBI has asserted that it needs that power to go after terrorists and criminals, critics say it would weaken digital security for everybody. The second part of the amendment would ban the NSA and FBI from accessing Americans' data without a warrant through a "loophole" in federal law, known as Section 702 of a 2008 update to the Foreign Intelligence

Events

June 16
Internet of Things: Securing the Government

Cyber Threats

OPM: Data Breach

FCC & FTC: Can they be harmonized?

ISSA DC Meetup

June 17
NovaInfosec Meetup

June 16 - 18
AFCEA Cyber Symposium

June 18
Telecom Cyber Risk Management

ISSA NoVA Meetup

Click here for detailed descriptions

Surveillance Act (FISA)."

-State lawmakers in California have approved legislation that would force law enforcement officers to obtain warrants or wiretap orders before searching digital devices including mobile phones and laptops, The Los Angeles Times reports. "The measure is supported by tech companies including Apple, Facebook, Google and Twitter as a way to clarify what their obligation is regarding providing information to law enforcement," writes Patrick McGreevy. "The bill is opposed by the California District Attorneys Assn., the California Police Chiefs Assn. and the California State Sheriffs Assn. as unnecessary and a burden to investigations."

Cyber Security Policy News

OPM breach update

-The previously disclosed data breach at The Office of Personnel Management which supposedly only affected 4 million government workers got a lot wider last week. Several publications, including The New York Times, Forbes and the Associated Press, printed stories quoting government union officials stating that the hack also jeopardized information on pretty much anyone who received or applied for a security clearance from the federal government.

The Times writes that The White House revealed that hackers had breached a second computer system at OPM, "putting at risk not only data about federal employees, but also information about friends, family members and associates that could number millions more." The story notes that President Obama is weighing sanctions against China, which multiple security firms have fingered as the source of the attack.

But Brendan Sasso at the National Journal raises the interesting question of whether the NSA spying scandal has left the U.S. without the moral high ground in the OPM hack. "The U.S. is an awkward position in deciding how to respond to the humiliating blow," Sasso writes. "That's partially because in the two years since Edward Snowden's leaks about U.S. surveillance, the Obama administration has repeatedly argued that hacking into computer networks to spy on foreigners is completely acceptable behavior." Read more here.

Airbus update

-Investigators have unearthed more details about what may have been responsible for the deadly crash of a military plane in Spain last month: Buggy software. "Plane-maker Airbus discovered anomalies in the A400M's data logs after the crash, suggesting a software fault," according to the BBC. "And it has now emerged that Spanish investigators suspect files needed to interpret its engine readings had been deleted by mistake."

Google and the "right to be forgotten"
Authorities in France are threatening Google with fines if it refused to apply Europe's "right to be forgotten" ruling to the search engine's global domains, including Google.com, observes the Electronic Privacy Information Center (EPIC). "Google has been reluctant to apply the landmark decisionbroadly, even after officials across Europe made clear that Google is violating the court judgement if it routinely discloses sensitive personal information to Internet users worldwide," EPIC argues. The New York Times' Bits blog has more on the controversy.

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