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

August 10, 2015

Two (2) events scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

-The U.S. Senate departed for its customary August recess without voting on a key cybersecurity bill. The National Journal reports that Senate Majority Leader Mitch McConnell withdrew the cyberinformation-sharing bill from consideration until September. "The bill-put forward by the top members of the Senate Intelligence Committee, Sens. Richard Burr and Dianne Feinstein-would offer incentives to the private sector to share information about cyberthreats with the government,"writes Kaveh Waddell. "Supporters, including senators from both parties and many in the private sector, say the information sharing legislation would make for stronger cyberdefenses against hackers. But privacy advocates in and out of the Senate have raised flags about the bill's treatment of Americans' sensitive information, saying it will violate personal privacy, and security experts have questioned the bill's effectiveness."

Cyber Security Policy News

Cell information update
-A federal court ruled last week that the U.S. government cannot obtain information about a cellphone's location without a warrant. The split decision from the 4th Circuit Court of Appeals concluded that warrantless searches of cellphone data are unconstitutional, writes The Hill. The

Events

August 11
NSA R&E Psyber Symposium

August 12-14
USENIX Security 2015

Click here for detailed descriptions

decision is being called a victory for privacy advocates who have sought new protections for people's information. Julian Hattem explains the back story leading up to this decision: "Cellphone providers such as AT&T and Verizon keep records whenever cellphones exchange radio waves with a local tower," Hattem writes. "Phones typically are in touch with their nearest cell tower, so a person's movement can effectively be tracked by looking at which towers a phone communicates with. Law enforcement officials relied in part on those types of records when they charged two men, Eric Jordan and Aaron Graham, in connection with a series of armed robberies in Baltimore five years ago. Police obtained court orders but not warrants to obtain location data about their phones covering a total of 221 days."

Pentagon email systems go offline after detecting a hack

-The Pentagon took its unclassified email systems offline after detecting an intrusion by alleged Russian hackers, NBC News reported last week. "According to the officials, the intrusion occurred sometime around July 25 and affected about 4,000 military and civilian personnel who work for the Joint Chiefs of Staff," NBC wrote. "The officials said the suspected Russian hackers coordinated the cyber attack via social media accounts. It's not clear whether the attack was sanctioned by the Russian government or was the work of individuals. The officials said that no classified information was seized or compromised and that only unclassified accounts and emails were hacked."

"Cybersecurity Sprint"

-The U.S. government conducted a so-called "cybersecurity sprint" last month aimed at improving Uncle Sam's security posture. According to the report, 72 percent of government computer users can only access networks there using a smart card. NextGov reports that while such progress is encouraging, it also means that more than a quarter of users need only a code to access untold terabytes of sensitive federal data.

New cyber law in the EU

-Tech and Internet companies like Amazon, Cisco and Google will need to adhere to a new law in the European Union that forces them to adopt tough security measures and report serious breaches to national authorities, according to Reuters. "The so-called Network and Information Security Directive has been stuck in talks between member states and EU lawmakers because of disagreements over whether to include digital platforms such as search engines, social networks, e-commerce sites and cloud computing providers," writesStephen Lam. "Members of the European Parliament want the law to only cover sectors they consider critical, such as energy, transport and finance. But after months of negotiations, digital platforms will now fall under the

law's remit, albeit with less onerous security obligations, according to the document, which did not provide details of the obligations."

China-based hackers hit health insurance and airlines

-There is evidence that a hacking group in China thought to be responsible for stealing tens of millions of records from U.S. health insurers also hacked American Airlines and Sabre Corp, which processes reservations for hundreds of airlines and thousands of hotels, Bloomberg reports. "Both companies were hacked as part of the same wave of attacks that targeted insurer Anthem Inc. and the U.S. government's personnel office, according to three people with knowledge of the cybersecurity probes," write Jordan Robertson and Michael Riley. "The investigators have tied those incursions to the same China-backed hackers, an assessment shared by U.S. officials, the people said. The latest incidents, which haven't previously been reported, are the broadest yet on the U.S. travel industry, emerging a week after security experts attributed an attack on United Airlines, the world's second-largest carrier, to the same group."

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