Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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

In This Issue

[Quick Links](#)

[Legislative Lowdown](#)

[Cyber Security Policy News](#)

[Events](#)

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

February 9, 2015

Eleven (11) Cyber security Events are scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

The Secure Data Act

-House lawmakers have introduced a measure that would bar the government from mandating access to technology products, The Hill reports. The Secure Data Act is 2015's iteration a House-passed amendment to the original Defense Department budget that didn't make it into the overarching 'cromnibus' budget passed late last year. The Senate and House also introduced versions of the measure in December," writes Cory Bennett. "The bill is part of the ongoing debate between the privacy community and law enforcement officials, who argue the rise of encryption that locks investigators out of devices such as iPhones could hinder legitimate efforts to thwart criminals and terrorists."

Search warrant for emails

-A bill that would require police to obtain a search warrant to read people's emails has broad support in the House, and is expected to garner equal support in the Senate, writes Julian Hattem for The Hill. "Under current law, which was passed in 1986, law enforcement officials don't need to

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman: @allanfriedman

obtain a warrant for emails, documents or items stored digitally in the cloud, as long as they are older than 180 days," Hattem explains. "Instead, they can nab the data with a subpoena, which does not come from a court and is often easier to obtain. Critics on both sides of the aisle say that's an unacceptable loophole and shows how the Electronic Communications Privacy Act has not kept up with the times. Activists from groups as varied as the Heritage Foundation and the American Civil Liberties Union have joined forces to push for an update."

Cyber Security Policy News

Anthem breach
-Anthem Inc., the nation's second largest health insurer,disclosed Wednesday that hackers had broken into its servers and stolen Social Security numbers and other personal data on up to 80 million Americans. The company says it does not believe the thieves took medical records or financial data, and that it will be notifying affected current and former Anthem members (formerly known as Wellpoint) by postal mail.

While the breach affects a large chunk of the American public, there are signs that the intruders were after information on very specific individuals to be used for cyber espionage purposes - not traditional cybercrime and identity theft, KrebsOnSecurity reports.

Crowdsourcing cybersecurity
-Companies and even the government routinely miss important clues about successful cyberattacks and data breaches until it's too late. Now, Silicon Valley entrepreneurs are talking about the idea of "crowdsourcing" cybersecurity. The Washington Post explains how this might work: "For one, there would be free and transparent sharing of computer code used to detect cyber threats between the government and private sector. In December, the U.S. Army Research Lab added a bit of free source code, a "network forensic analysis network" known as Dshell, to the mega-popular code sharing site GitHub," The Post's Dominic Basulto explains. "Already, there have been 100 downloads and more than 2,000 unique visitors. The goal, says William Glodek of the U.S. Army Research Laboratory, is for this shared code to "help facilitate the transition of knowledge and understanding to our partners in academia and industry who face the same problems." Read more here.

TurboTax: account takeovers
-TurboTax owner Intuit Inc. said last week that it was temporarily suspending the transmission of

state e-filed tax returns in response to a surge in complaints from consumers who logged into their TurboTax accounts only to find crooks had already claimed a refund in their name. The company later resumed state filing, saying an investigation revealed no evidence that TurboTax was compromised, and experts say the spike in fraud is likely due to consumers having their email accounts and computers compromised. In either case, TurboTax said it was adding two-step authentication to all accounts to help prevent account takeovers.

Silk Road "kingpin" convicted

-The man the U.S. government arrested last year and charged with operating the online black market known as the Silk Road has been convicted on all seven counts, Wired reports. "On Wednesday, less than a month after his trial began in a downtown Manhattan courtroom, 30-year-old Ulbricht was convicted of all seven crimes he was charged with, including narcotics and money laundering conspiracies and a 'kingpin' charge usually reserved for mafia dons and drug cartel leaders," writes Andy Greenberg. "It took the jury only 3.5 hours to return a verdict. Ulbricht faces a minimum of 30 years in prison; the maximum is life. But Ulbricht's legal team has said it will appeal the decision, and cited its frequent calls for a mistrial and protests against the judge's decisions throughout the case."

Requested $14 billion for network improvements

-President Obama's 2016 budget proposal requests some $14 billion to beef up protection of government and private networks from cyberattacks. The budget calls for additional intrusion detection and prevention ability, increased information sharing between the public and private sectors, and improved attack response. Reuters has a deeper breakdown.

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