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

October 6, 2014

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

Announcements

How corporations are protecting data

CSPRI Research Scientist, Dr. Allan Friedman, speaks with CCTV about data breaches. Click here to see the clip!

Cyber Security Policy News

JPMorgan Update

-Hackers who broke into Wall Street bank JPMorgan Chase & Co. earlier this year made off with data on more than 76 million households and 7 million small businesses, the company said in a corporate filing last week. Business Week reports that the hackers exploited an employee password to crack a JPMorgan server and ultimately pull off one of the largest cyber-attacks ever. "JPMorgan, the largest U.S. bank, outlined the scope of the previously disclosed breach yesterday, reassuring clients there's still no evidence account numbers and passwords were compromised, even

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

CSPRI in the News

In Politico

CSPRI Research Scientist, Dr. Allan Friedman was featured in Politico in their "Cyber Month of Misconceptions" in honor of National Cybersecurity Awareness Month.

Read the story here.

Follow Us

Follow us on Twitter: @gwCSPRI

as names and contact data were exposed," wrote Hugh Son and Michael Riley. "People who logged on to certain websites or mobile apps had contact information stolen, the New York-based company said." A copy of that corporate filing is here.

The break-in at JPMorgan has prompted investigations by at least two state attorneys general, Reuters reports. "Illinois Attorney General Lisa Madigan said she has launched a probe into the hack on the No. 1 U.S. bank by assets," Jim Finkle and Karen Freifeld wrote. "Connecticut is also investigating, said a person familiar with the matter who was not authorized to publicly discuss the probe."

Speaking on CBS's 60 Minutes Sunday night, FBI Director James Comey called cyber attacks an "epidemic." "Cybercrime is becoming everything in crime," Comey said. "Again, because people have connected their entire lives to the Internet, that's where those who want to steal money or hurt kids or defraud go. So it's an epidemic for reasons that make sense."

ComputerCOP

-A popular program marketed as a way to help parents protect their children from online predators may actually be putting those families' privacy at risk, according to a report published by the Electronic Frontier Foundation. The EFF looked at ComputerCOP, a software title that has become so popular that local police forces nationwide hand it out free to concerned parents. But as the National Journal reports, the EFF analysis of the program found no evidence that the program is keeping kids safe. "Instead, the report says, it serves as de facto spyware that takes private computer data and puts it online with woefully inadequate protections."

Meanwhile, the U.S. attorney general urged technology companies to preserve law-enforcement access to smartphone data, responding to new privacy features from Apple Inc. and Google Inc. that he said would hamper investigations of child sex abuse. "Holder said today in prepared remarks he hoped the industry would co-operate ensure (sic) that authorities can still get information with court approval from mobile devices," the Globe and Mailreports. "His comments echo concerns from other law enforcement officials that the companies' new privacy policies will stymie inquiries into crimes ranging from drug trafficking to terrorism."

Vulnerability in flash drives

-A serious security hole present in most USB flash drives allows the devices to be infected with insidious, undetectable malicious software, according to Wired.com. Researchers first presented their findings - which they dubbed "Bad USB" -- this summer at the Black Hat security convention in Las Vegas, but they declined to release details of the exploit. This past week, however, instructions showing exactly how the flaw can be exploited were posted online. "In a talk at the Derbycon hacker conference in Louisville, Kentucky last week, researchers Adam Caudill and Brandon Wilson showed that they've reverse engineered the same USB firmware as Nohl's SR Labs, reproducing some of Nohl's BadUSB tricks," writes Wired's Andy Greenberg. "And unlike Nohl, the hacker pair has also published the code for those attacks on Github, raising the stakes for USB makers to either fix the problem or leave hundreds of millions of users vulnerable.

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman: @allanfriedman

FDA guidelines for medical devices

-The Food & Drug Administration has issued long-awaitedguidelines on the cybersecurity of medical devices, USA Today writes. "The agency is recommending that manufacturers consider cybersecurity risks as they design and develop medical devices," reports Elizabeth Weise. "Further, companies should give the FDA information about the potential risks they found and what controls they put in place to mitigate them." The regulatory agency says it expects to hold a national workshop on medical devices and cybersecurity on Oct. 21 and 22.

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
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052