Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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 8, 2015

Seven (7) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

-The U.S. Senate voted last week to approve the long-debated USA Freedom Act, formally ending one of the government's most controversial surveillance programs involving the collection of US phone records. Wired.com reports on the vote, which passed 62 to 32. "The legislation puts an end to the NSA's bulk collection of phone records by having telecoms store the records instead," writes Kim Zetter. "The legislation would still allow the government to access the records, by obtaining a court order from the Foreign Intelligence Surveillance Act any time it wishes to view them, but would limit this access to records that are relevant to a national security investigation." Read more.

Cyber Security Policy News

OPM breach
-The Office of Personnel Management disclosed last week that a breach involving hackers apparently originating from China exposed the personal data on some 4 million current and former employees. The news sent lawmakers scrambling to compose statements decrying the incident as another state-sponsored attack on America. According to The New

Events

June 8-11
Security and Risk Summit

June 9
Exploit migration techniques by Microsoft

June 10
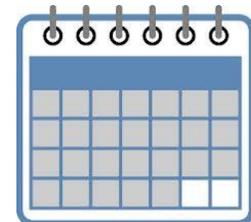Reducing IT Acquisition Risk

June 10
NovaInfosec

June 10-13
NIST Board Meeting

June 11
ISACA NCA Meetup

June 16-18
Defensive Cyber Operations

Click here for detailed descriptions

York Times, the hack was tied to the same group thought to be responsible for hacking into and stealing 80 million records from healthcare provider Anthem and some 13 million records from Premera, among other providers.

NextGov reports that months before the OPM's most recent data breach, the agency had requested an additional $32 million for the 2016 fiscal year -- much of which was slated for strengthening network security, budget justification shows.

Airbus crash caused by faulty software
-An executive of Airbus Group has confirmed that the crash of an Airbus A400M military transport was caused by a faulty software configuration. "Marwan Lahoud, chief marketing and strategy officer for Airbus, told the German newspaper*Handelsblatt* on Friday that there was a 'quality issue in the final assembly' of the components of the aircraft engine," writes Sean Gallagher for Ars Technica. Read more of the reporthere.

NSA update
-While attention moves to the House to debate and vote on legislation passed by the Senate to curtail the NSA's domestic surveillance activities, documents newly leaked by former NSA contractor Edward Snowden reveal a continued expansion of cybersurveillance activities by U.S. agencies. The New York Times posted excerpts from the documents, which it saidprovided fresh evidence that "without public notice or debate, the Obama administration has expanded the NSA's warrantless surveillance of Americans' international Internet traffic to search for evidence of malicious computer hacking."

Bitcoin guidelines
-Bitcoin, an increasingly popular virtual currency that has also become the de facto lingua franca of the cybercrime underground, is receiving some new scrutiny from federal regulators. "A top Wall Street watchdog on Wednesday issued new rules that place stricter cybersecurity requirements on financial firms wishing to use virtual currencies," writes Cory Bennett for The Hill. "Under the guidelines, financial firms handling bitcoins and other digital currencies will need to obtain a 'BitLicense' from the NYDFS, ensure a strong cyber defense and maintain detailed records of all bitcoin transactions."

China's "Great Firewall"
- Getting a virtual private network connection from within China to the outside Internet beyond China's "Great Firewall" censorship program just got a bit harder. According to The Register, "China's government is cracking down further on the use of virtual private networks to circumnavigate its Great Firewall, as part of the ongoing game of whack-a-mole between censors and an increasingly tech-savvy population." The Register's Kat Hall has

more [here](#).