October 17, 2017

Hacking Healthcare

TLP White
Welcome back to *Hacking Healthcare!* You will now be seeing us at a regularly scheduled time – every Tuesday morning.

Hot Links –

1. Hack Back Fever – A bipartisan bill was introduced in the House last week, which if passed would enable companies to take action against cyber attackers. The bill would amend the Computer Fraud and Abuse Act to prohibit prosecution against network defenders who act outside of their networks to disrupt ongoing attacks or conduct reconnaissance for purposes of attribution or network defense. The bill would require that an organization notify the FBI before taking any action – a time lag which may limit the effectiveness of disruptive defensive operations. And it would only enable defensive measures against infrastructure located in the United States (which law enforcement already can take action against). If a U.S. person (or their computers) were harmed during a hack-back, the bill would enable private action to seek damages.

   There are also portions of the bill that clarify the legality of beaconing implants that might help establish attribution. This seems like firmer ground to start on as we better develop standards for attribution and increase law enforcement capacity in the U.S. and overseas.

2. HIMSS likes Cyber – This year, HIMSS' top "Congressional Ask" is for a designated HHS Cyber Lead. It looks like NH-ISAC and HIMSS are on the same page. HIMSS recommend that the HHS CISO be this "lead" and focus not only on HHS security but also on developing better support of the sector through information sharing and cyber outreach and training.

3. More Breaches – Another example of a company that stored patient data in the cloud, and then did nothing to secure it. A good reminder that you can outsource certain functions, but not the responsibility to institute security controls.

4. DHS gets secure – Jeannette Manfra, Assistant Secretary at DHS, announced a new requirement that all Federal agencies use HTTPS and DMARC. Good to see the government is eating their vegetables.

5. More Cyber – Rob Joyce, the cybersecurity lead within the White House and NSC, is now also the Deputy Homeland Security Advisor. This job has primary responsibility over response to physical emergencies, such as natural disasters and active shooter situations. It's unclear whether this is meant to fill a short-term gap in personnel or if it is a realignment meant to bring cyber and physical resiliency closer together.

Congress – The House is out of town this week, but the Senate has a couple of interesting hearings scheduled:

Tuesday, October 17:
--Hearing: Consumer Data Security and the Credit Bureaus (Senate Banking)

Thursday, October 19:
--Hearings to examine the roles and responsibilities for defending the Nation from cyber attack (Senate Armed Services)

Thursday, October 26:
--Hearings to examine advanced cyber technologies that could be used to help protect electric grids and other energy infrastructure from cyberattacks (Senate Energy)

Monday, October 30:
--Hearing: Examining Physical Security and Cybersecurity at Our Nations Ports (House Homeland)

Conferences and Webinars –
--EDGE 2017 – Knoxville (10/17-18)
--Boston CISO Roundtable – Boston (IANS) (10/18)
--Health IT Summit – Raleigh (NH-ISAC) (10/19)
--NIST IoT Cybersecurity Colloquium (10/19)
--Business E-mail Compromise (BEC) Workshop – Kennedy Space Center (NH-ISAC) (10/19)
--Business E-mail Compromise (BEC) Workshop – Akron (NH-ISAC) (10/25)
--Business E-mail Compromise (BEC) Workshop – Phoenix (NH-ISAC) (10/26)
--Business E-mail Compromise (BEC) Workshop – Denver (NH-ISAC) (10/27)
--Business E-mail Compromise (BEC) Workshop – Nashville (NH-ISAC) (10/30)
--Biotec/Pharma Security Workshop at MSD, Prague (NH-ISAC) (11/7)
--Health IT Summit – LA (NH-ISAC) (11/9)
--Cyber Outbreak (NH-ISAC) (11/27)
--NH-ISAC Fall Summit – Cyber Rodeo (11/28-30)
--Health IT Summit – Dallas (NH-ISAC) (12/14)

October 17, 2017

Sundries –

--The World Once Laughed at North Korean Cyberpower. No More. (NYT)
--Herb Lin: The Real Threat from Kaspersky Security Software (Lawfare)
--Deputy AG Rosenstein: Remarks on Encryption
--How one contractor (Oracle) belittled the White House's IT modernization strategy (Federal News Radio)
--Podcast: Medical Devices (Cyber Chat – Federal News Radio)
--Iranian hackers compromised the UK leader Theresa May's email account along with other 9,000 emails (Security Affairs)
--Severe flaw in WPA2 protocol leaves Wi-Fi traffic open to eavesdropping (Ars)
--Hackers use organizations' resources for stealthy cryptocurrency mining (HelpNet)
--Locky Skyrockets Up Global Malware Rankings (info security)
--Australian defense firm was hacked and F-35 data stolen, DOD confirms (Ars)
--Supreme Court agrees to hear DOJ petition in Microsoft data warrant case (the Hill)

Contact us: follow @NHISAC and email at bflatgard@nhisac.org