February 13, 2018

Hacking Healthcare

TLP White
This week we continue to look at GDPR, as well as the federal government budget, and Olympic mania:

Hot Links –

1. ***Google gets Aggressive:*** I'm a fan of simple and intuitive security disclosures that can inform (or nudge[1]) *the market* to reward good security practices. Google Chrome's move towards more intuitive and visible markings for unencrypted web traffic is a good step in the right direction.[2] Tinder better catch-up![3]

2. ***Olympic Destroyer:*** It looks like the Olympic organizers dodged a bullet ahead of the opening ceremony. Talos says that the purpose of the attack was disruption and destruction – rather than any attempt at theft. "The destructive nature of this malware aims to render the machine unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment."[4]

3. ***Budgets:*** Last Friday, the President signed a two-year spending bill into law.

   This week, the White House released a proposal for its next budget.[5] While the proposal included big spending cuts across the board – security spending got some bumps. The budget proposes a significant increase in the DHS office that handles critical infrastructure security and federal network security.[6]

   That being said, Treasury, Education, Energy[7], and Interior all had proposals to increase their ability to support the cybersecurity of key critical infrastructure. HHS didn't get any of the same attention. What gives?

[1] https://www.theverge.com/2018/2/8/16991254/chrome-not-secure-marked-http-encryption-ssl
[2] https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html
[3] https://www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/
[4] http://blog.talosintelligence.com/2018/02/olympic-destroyer.html
[5] https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf
[6] http://thehill.com/policy/cybersecurity/373457-trump-requests-33-billion-for-homeland-security-cyber-unit-in-2019
[7] https://www.cyberscoop.com/department-of-energy-cybersecurity-office-ceser/

No one believes this proposal will be adopted by Congress. But it does serve an important role in signaling the Administration's priorities. The new HHS Secretary is due to defend the proposal in a hearing on Wednesday morning. Let's see if he talks cyber.

4. ***GDPR:*** As we started to discuss last week, GDPR is the new *General Data Protection Regulation* that comes into effect on May 25. GDPR establishes the rights of European residents in relation to their *personal data.* It is designed to protect the privacy of European citizens and residents – and in doing so impacts all organizations that are located in Europe or that collect or store the information of European residents.

   GDPR pertains not only to how an organization must protect information and notify impacted parties in the event of a breach, but also when and how it is permissible for an entity to collect, store, and process *personal data*.

   Personal data is the broad term under GDPR for "any information relating to an identified or identifiable natural person (data subject)." This is a more inclusive definition than PII in the U.S. – a name or even an IP address can constitute *personal data* under the GDPR.

   Health data is given special consideration under the GDPR.[8] Under the regulation there is a default prohibition against processing health data – which includes "data concerning health,"[9] biometric data, and genetic data. To process health data certain conditions must be met. One condition is for the data subject to provide "explicit consent." This is the strongest grounds for an organization to stand on – and is somewhat like the provisions requiring disclosure and affirmative consent within HIPAA. There are further conditions where health data can be processed – most notably when "processing is necessary for the purposes of preventive or occupational medicine."[10]

   GDPR sets an expectation that organizations will report any breaches very quickly – "without undue delay and, where feasible, not later than 72 hours after becoming aware of it" – to the relevant national supervisory authority. There is a further obligation to notify the data subject without undue delay.

   Similar to OCR's view, ransomware may constitute a data breach that requires reporting under GDPR[11] unless an organization can demonstrate that the ransomware attack "is unlikely to result in a risk to the rights and freedoms of natural persons."[12]

   Next week we will continue looking at European data protections including strategies for healthcare organizations to prepare for GDPR. We'll also take a look at the EU-US

[8] https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A9

[9] "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[9]

[10] Article 9, Paragraph 2.8

[11] *Definitions*, from Article 4, paragraph 12: "'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

[12] https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#R85

Privacy Shield, which governs how U.S. businesses can transit data to and from the European Union and maintain compliance with European regulations. It is an important corollary regulation to GDPR.

And if you want to get further into GDPR, you can sign-up for the NH-ISAC members-only webinar on March 13: <https://nhisac.org/events/nhisac-events/nh-isac-gdpr-101/>

Congress –

Tuesday, February 13:
--Hearings to examine worldwide threats (Senate Intel)[13]

Wednesday, February 14:
--Hearing on the Department of Health and Human Services' Fiscal Year 2019 Budget Request (House Ways and Means)[14]
--Hearing: Examining the Current Data Security and Breach Notification Regulatory Regime (House Financial Services)[15]
--Hearing: Beyond Bitcoin: Emerging Applications for Blockchain Technology (House Science)[16]
--Hearing: Examining the Impact of Health Care Consolidation (House Commerce)[17]
--Hearing: GAME CHANGERS: ARTIFICIAL INTELLIGENCE PART I (House Oversight)[18]

Thursday, February 15:
--Hearing: Oversight of the Department of Health and Human Services (House Commerce)[19]

Conferences and Webinars –

--"Unbirden" Your Inbox - Perch Security – Webinar (2/15) <https://nhisac.org/events/nhisac-events/perch-security/>
--Third Party Risk Webinar (2/21) <https://nhisac.org/events/nhisac-events/member-third-party-risk-webinar/>
--NH-ISAC GDPR 101 Webinar (3/13) <https://nhisac.org/events/nhisac-events/nh-isac-gdpr-101/>
--Basic Best Practices in Cybersecurity – Alabama (2/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-alabama/>
--InfoSec World – Orlando (3/19) <https://nhisac.org/events/nhisac-events/infosec-world/>

[13] https://www.intelligence.senate.gov/hearings/worldwide-threats-hearing
[14] https://waysandmeans.house.gov/event/hearing-department-health-human-services-fiscal-year-2019-budget-request/
[15] https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402988
[16] https://science.house.gov/legislation/hearings/subcommittee-oversight-and-subcommittee-research-and-technology-hearing-beyond
[17] https://energycommerce.house.gov/hearings/examining-impact-health-care-consolidation/
[18] https://oversight.house.gov/hearing/game-changers-artificial-intelligence-part/
[19] https://energycommerce.house.gov/hearings/oversight-department-health-human-services/

--Medical Device Workshop at Philips Healthcare – Andover, MA (3/20) <https://nhisac.org/events/nhisac-events/medical-device-workshop-at-philips-healthcare-andover-ma/>

--Health IT Summit – Cleveland, OH (3/27) <https://vendome.swoogo.com/2018-Cleveland-Health-IT-Summit>

--Health IT Summit – San Francisco, CA (4/5) <https://vendome.swoogo.com/2018-San-Francisco-HIT-Summit>

--Security Workshops at Intermountain Health – Park City, UT (4/24) <https://nhisac.org/events/nhisac-events/security-workshop-at-intermountain-park-city-ut/>

--Medical Device and Pharmaceutical Security Workshop – London <https://nhisac.org/events/nhisac-events/security-workshops-london/>

--2018 NH-ISAC Spring Summit – Sawgrass, FL (5/14-17) <http://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>

--Health IT Summit – Philadelphia, PA (5/21) <https://vendome.swoogo.com/2018-Philly-HITSummit>

--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>

--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21) <https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>

--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>

--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>

--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>

--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>

--Biotech/Pharma Security Workshop at Gilead Sciences, Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>

--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>

--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

--**Business Associate Dismissal Denied in HIPAA Data Breach Case** <https://healthitsecurity.com/news/business-associate-dismissal-denied-in-hipaa-data-breach-case>

--**Tennessee Hospital Hit with Cryptocurrency Mining Malware** <https://www.darkreading.com/attacks-breaches/tennessee-hospital-hit-with-cryptocurrency-mining-malware/d/d-id/1331014>

February 13, 2018

--**Now Cryptojacking Threatens Critical Infrastructure, Too**
<https://www.wired.com/story/cryptojacking-critical-infrastructure/>
--**Radiflow Reveals First Documented Cryptocurrency Malware Attack on a SCADA Network**
<https://www.prnewswire.com/news-releases/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network-300595714.html>
--**U.S. Secretly Negotiated with Russians to Buy Stolen NSA Documents**
<https://theintercept.com/2018/02/09/donald-trump-russia-election-nsa/>
--**Timothy Noonan Named OCR Acting Deputy Director**
<https://healthitsecurity.com/news/timothy-noonan-named-ocr-acting-deputy-director>
--**VA OIG finds cybersecurity flaws at Orlando VA Medical Center**
<http://www.healthcareitnews.com/news/va-oig-finds-cybersecurity-flaws-orlando-va-medical-center>
--**Necurs Spammers Go All In to Find a Valentine's Day Victim**
<https://securityintelligence.com/necurs-spammers-go-all-in-to-find-a-valentines-day-victim/>

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