November 21, 2017

Hacking Healthcare

TLP White

One man's vulnerabilities are another man's exploits: bugs: bounties – this week's *Hacking Healthcare:*

Hot Links –

1. **First, a little of our own cyber-hygiene:** This past week, Ed Brennan, Ops Director at NH-ISAC, gave me a friendly reminder that embedding links in emails is *NOT* an NH-ISAC approved best practice! The idea being that malicious links may be foisted upon unsuspecting recipients.

   We would like to set a good example here and prove that killing hyperlinks can help mitigate cyber-risk while being user friendly. So we will move to footnoting any linked articles or reports. We would also recommend that organizations go beyond this measure and move to whitelist applications (See: a NIST guide to that[1]) to further protect against hazardous web-browsing and link clicking. Let us know how you get on with this or if you have recommendations on secure user-friendly practices.

2. **Vulnerabilities under review:** This past week, Rob Joyce (White House Cyber Czar) publicly released[2] a newly revised process[3] by which the government decides whether to disclose computer vulnerabilities that it discovers. Known as the *Vulnerability Equities Process,* the new charter is most notable for the fact that it is now public.

   The long shadow of public distrust cast by the Snowden leaks should inform any analysis of this new policy. Some[4] will criticize the VEP charter as not going far enough. Many believe that the government should responsibly disclose all vulnerabilities discovered in

[1] <https://www.nist.gov/news-events/news/2015/11/nist-offers-guidance-using-technology-prevent-intrusions-malware >

[2] <https://www.whitehouse.gov/blog/2017/11/15/improving-and-making-vulnerability-equities-process-transparent-right-thing-do>

[3] <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>

[4] Schneier has a passionate take: <https://www.schneier.com/blog/archives/2017/11/new_white_house_1.html>

commercial products. Others think a patch should be developed alongside exploits. These are worth discussion, though the distrust caused by Snowden (and the government’s messy response) tends to poison any clear-eyed debate about what approach best balances intelligence collection, disruptive cyber-operations, and national defense.

I applaud the release of the charter as a good faith effort to better engage citizens and critical infrastructure operators in the process of national cyber defense. Rather than bemoan its shortcomings, we should look at this as the starting point in a process. Informing the government as to why changes might be necessary is the role of critical infrastructure sectors.

At this point, it seems most important to focus any critique on the structural approach of the process. If the main purpose is to provide documented and accountable cost benefit analysis of any vulnerabilities, the data being analyzed and the people responsible for the analysis are of primary import.

The benefit of vulnerabilities is relatively easy to calculate – you point to intelligence collected or accesses gained. Quantifying the downside risk of unpatched vulnerabilities being exploited is more difficult. There is a probabilistic debate over likelihood that an adversary has discovered the vulnerability. One must also point to an adversary’s intent to utilize such a vulnerability against a certain target – it is difficult to accomplish explicit attribution of such intent.

But even more challenging is understanding the impact to critical infrastructure if a vulnerability is exploited. Many companies cannot tell you the impact within their own business if a certain technology were to be exploited. This becomes more challenging when applied on a national scale and without understanding of commercial technology deployments or network architectures. The government simply doesn’t have the data.

Yet the private sector is not invited to participate in the discussion. The “Equities Review Board,” which is established in the charter, is comprised of government agencies. The usual players are there from law enforcement and the intelligence community, as well as some civilian representatives such as the Departments of Commerce, Treasury, and Energy.

One important (and notable) admission from the government stakeholder group which determines the release of vulnerabilities – Health and Human Services. HHS does not have the historical involvement in national security that Treasury or Energy do (two sector specific agencies included in the process), but determining impact of vulnerabilities on the health sector seems squarely within their remit.

3. **Bugs** - Speaking of vulnerabilities, bug bounties are becoming ever more popular. Hacker One[5] and Bugcrowd[6] have recently put out reports on the state of the bug bounty industry. The Hacker One report says that only 3 percent of its bounty programs are run by companies in the healthcare sector. Why is that?

   Also of note – healthcare is at least twice as likely to be vulnerable to SQL injection as other industries in the study.

4. **More Bills!** – This time "Bill of Materials." Rep. Greg Walden (R-Oregon) recently sent a letter[7] to HHS asking that the Secretary convene a group this year[8] to implement one of the Healthcare Cybersecurity Task Force recommendations – ship medical devices with a Bill of Materials.

Congress – Congress is at home this week.

Conferences and Webinars –

--Cyber Outbreak TTX (NH-ISAC) (11/27) <https://nhisac.org/events/nhisac-events/cyber-outbreak-cybersecurity-tabletop-exercise/>
--NH-ISAC Fall Summit – Cyber Rodeo (11/28-30) <https://nhisac.org/events/cyber-rodeo/>
--2017 Third Party Risk Governance Summit (11/30-12/1) <https://nhisac.org/events/2017-tprg-summit/>
--Business Email Compromise Workshop – New York, NY (12/5) <https://nhisac.org/events/nhisac-events/business-e-mail-compromise-workshop/>
--Regional Healthcare Cybersecurity Summit – Hebron, KY (12/7) <https://nhisac.org/events/nhisac-events/regional-healthcare-cybersecurity-summit/>
--Basic Best Practices in Cybersecurity – Georgia (NH-ISAC) (12/13) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-georgia/>
--Health IT Summit – Dallas (12/14) <https://vendome.swoogo.com/Dallas-HITSummit-2017>

Sundries –

--Intel Chip Flaws Leave Millions of Devices Exposed <https://www.wired.com/story/intel-management-engine-vulnerabilities-pcs-servers-iot/>
--Adobe, Microsoft Patch Critical Cracks <https://krebsonsecurity.com/2017/11/adobe-microsoft-patch-critical-cracks/>

[5] < https://www.hackerone.com/resources/hacker-powered-security-report>
[6] < https://arstechnica.com/information-technology/2017/11/bugcrowd-unmasks-sort-of-hackers-to-cast-vulnerability-hunters-in-better-light/>
[7] < https://energycommerce.house.gov/wp-content/uploads/2017/11/20171116HHS.pdf>
[8] <https://healthitsecurity.com/news/healthcare-cybersecurity-threats-require-hhs-bill-of-materials>

November 21, 2017

--What to know about the FCC's upcoming plan to undo its net neutrality rules <https://www.washingtonpost.com/news/the-switch/wp/2017/11/20/what-to-know-about-the-fccs-upcoming-plan-to-undo-its-net-neutrality-rules/?utm_term=.1883cba93fbf>
--Senator urges ad blocking by feds as possible remedy to malvertising scourge <https://arstechnica.com/information-technology/2017/11/senator-urges-ad-blocking-by-feds-as-possible-remedy-to-malvertising-scourge/>
--No, you're not being paranoid. Sites really are watching your every move < https://arstechnica.com/tech-policy/2017/11/an-alarming-number-of-sites-employ-privacy-invading-session-replay-scripts/>
--Why Google should be afraid of a Missouri Republican's Google probe < https://arstechnica.com/tech-policy/2017/11/conservative-backlash-a-missouri-republican-is-investigating-google/>
--Pentagon contractor leaves social media spy archive wide open on Amazon <https://arstechnica.com/information-technology/2017/11/vast-archive-from-pentagon-intel-gathering-operation-left-open-on-amazon/>
--CompuServe Forums, RIP <https://arstechnica.com/information-technology/2017/11/compuserve-forums-rip/>

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