August 21, 2018

Hacking Healthcare

TLP White

We start with an effort by Chinese hackers to gain a competitive trade advantage and then turn to President Trump's move towards a more offensive cyber strategy. We conclude with addressing security gaps in Maryland's Medicaid Management Information System. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Chinese Cyber-Recon on U.S. Properties Exposed.*** Cyber threat intelligence provider Recorded Future reported that hackers from China's Tsinghua University targeted several geopolitical organizations, including the State of Alaska Government and Alaska's Department of Natural Resources.[1] The network reconnaissance activities identified by Recorded Future occurred before and after a U.S. trade delegation visit to China in May of this year.[2]

   The visit was led by Alaskan governor Bill Walker and involved representatives of companies and economic development agencies in an effort to explore economic development opportunities in China. The report revealed that hackers used computers at Tsinghua to target U.S. energy and communications companies, as well as the Alaskan state government. Further, the report explains that the hackers targeted computer systems that belong to Alaska Communications, the state Department of Natural Resources, Alaska Power and Telephone, TelAlaska, and the governor's office. The hackers were likely searching for security flaws and vulnerabilities that would enable access confidential systems. Fortunately, there is no evidence to support that the hackers were able to compromise or access information from any Alaska computers.[3]

2. ***Trump Nixes PPD-20 and Empowers Offensive Cyber Capabilities.*** The President rescinded an Obama era order, known as Presidential Policy Directive 20 ("PPD-20)") in

[1] https://go.recordedfuture.com/hubfs/reports/cta-2018-0816.pdf

[2] https://www.reuters.com/article/us-usa-china-cyber/chinese-hackers-targeted-u-s-firms-government-after-trade-mission-researchers-idUSKBN1L11D2

[3] https://www.usnews.com/news/best-states/alaska/articles/2018-08-17/report-chinese-hackers-targeted-alaska-networks

an effort to reduce restrictions on how and when the U.S. government can deploy cyberweapons against adversaries.[4] PPD-20 established an extensive interagency process which was required prior to initiating cyberattacks against foreign adversaries. Now, the military has more flexibility to deploy hacking tools without pushback from government and without sign-off from the White House for individual strikes.

The problem with the debate around offensive vs. defensive approaches is that it does not account for other strategies for managing cyber conflict, a problem greatly exacerbated by the fact that no real norms of behavior exist for war in cyberspace[5]. Without norms, determining when offensive cybersecurity actions are appropriate will be at every countries discretion. We have previously discussed private sector parallels to this issue when looking at the notion of companies "hacking back". The example that the US government sets in the use of offensive capabilities may well influence future legislation around what companies can do to each other.

It is yet to be seen if the Trump Administration will replace PPD-20 with other directives, or leave it solely in the hands of Cyber Command.

3. ***Security Gaps in MD Medicaid Management Information System.*** A recent audit conducted by the Department of Health and Human Services ("HHS") revealed that Maryland's Medicaid program has several security gaps which threaten exposure of data and information systems to unauthorized parties as well as disruption of critical operations.[6] According to the HHS assessment, the Medicaid Management Information System ("MMIS") suffered from a large number of system vulnerabilities, resulting from a failure to implement sufficient controls over MMIS data and systems.

   Maryland is not by itself in the category of states with poor information security practices in the healthcare sector. Virginia, Alabama, North Carolina, and Massachusetts all received poor grades for security implementation last year. This can in part be explained by the slow adoption of new or updated cybersecurity practices, the use of older operating systems, and failure to apply patches and updates to installed software.

   The HHS report on Maryland indicated that the vulnerabilities were severe, but that there was no evidence that they were leveraged by malicious actors. HHS made their point loud and clear, and Maryland has accepted several proposed recommendations, guidance, and remediation actions.

Congress –

[4] https://www.cyberscoop.com/ppd-20-eliminated-cyber-war-donald-trump-mike-rounds/

[5] https://www.justsecurity.org/53329/outlook-international-cyber-norms-avenues-future-progress/

[6] https://www.bleepingcomputer.com/news/security/severe-security-gaps-in-marylands-medicaid-management-information-system/

Tuesday, August 21:
--Hearing to examine Centers for Medicare and Medicaid Services efforts to fight Medicaid fraud and overpayments (Senate Committee on Homeland Security and Governmental Affairs).[7]
--Hearing to examine the energy efficiency of blockchain and similar technologies and the cybersecurity possibilities of such technologies for energy industry applications (Senate Committee on Energy and Natural Resources).[8]
--Hearing to examine cyber threats to our nation's critical infrastructure (Senate Subcommittee on Crime and Terrorism).[9]

Wednesday, August 22:
--No relevant hearings

Thursday, August 23:
--Hearing to examine prioritizing cures, focusing on science and stewardship at the National Institutes of Health (Senate Committee on Health, Education, Labor, and Pensions).[10]

Conferences, Webinars, and Summits –

--NH-ISAC Blended Threats Exercise Series – No. CA (8/28) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--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/>
--Basic Best Practices in Cybersecurity – Abilene, KS (8/29) https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-kansas-3/
--NH-ISAC Radio - Cybersecurity Design Engineering for Medical Devices (Member-only link on member listerver) 8/31 Noon ET
--Basic Best Practices in Cybersecurity – Granite Falls, MN (9/5) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-granitefalls-mn/>
--NH-ISAC Blended Threats Exercise Series – DE (9/10) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Basic Best Practices in Cybersecurity – Nashville, TN (9/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-nashville/
--NH-ISAC Blended Threats Exercise Series – GA (10/2) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

[7] https://www.senate.gov/committees/hearings_meetings.htm
[8] https://www.senate.gov/committees/hearings_meetings.htm
[9] https://www.senate.gov/committees/hearings_meetings.htm
[10] https://www.senate.gov/committees/hearings_meetings.htm

--Information Sharing Turns 20: Learn more at Borderless Cyber USA – Washington, DC (10/4) <https://nhisac.org/events/nhisac-events/information-sharing-turns-20-learn-more-at-borderless-cyber-usa/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--CSS - "Table Stakes" in the Development and Deployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>
--Summit on Third-Party Risk – Leesburg, VA (10/24-26) <https://nhisac.org/events/nhisac-events/summit-on-third-party-risk/>
--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>
--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>
--NH-ISAC Blended Threats Exercise Series – So. CA (11/19) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

--**DHS holds election security exercise with states to prep for midterms** <https://www.cyberscoop.com/dhs-election-security-exercise//>
--**Academics Discover New Bypasses for Browser Tracking Protections and Ad Blockers** <https://www.bleepingcomputer.com/news/security/academics-discover-new-bypasses-for-browser-tracking-protections-and-ad-blockers/>
--**Microsoft Office For Windows Updated With New Features for Insiders** <https://www.bleepingcomputer.com/news/microsoft/microsoft-office-for-windows-updated-with-new-features-for-insiders/>
--**Instagram Hack: Hundreds Affected, Russia Suspected** <https://www.darkreading.com/attacks-breaches/instagram-hack-hundreds-affected-russia-suspected/d/d-id/1332558>
--**Report: 'Faxploit' hack can penetrate networks with just a fax number** <https://www.cyberscoop.com/faxploit-check-point-technologies/
Contact us: follow @NHISAC and email at contact@nhisac.org