October 13th, 2020

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* takes a look at how risk management is evolving with the increase of remote work. We start by revisiting the long running Huawei saga to give you an update on a new report from the United Kingdom's Parliament that is bound to antagonize the Chinese government and potentially lead to reprisals. Next, we briefly examine the United States Cybersecurity and Infrastructure Security Agency's (CISA) release of guidance for ransomware and telework that could be a useful comparative reference for healthcare organizations. Finally, we dig into a new report on the state of endpoint and Internet of Things (IoT) security with an eye towards how some of the more interesting findings may apply to the healthcare sector. ***Please give us a minute of your time to answer a few questions about this week's Hacking Healthcare topics. We'll publish the results in an upcoming issue. Survey link follows the articles below.***

Welcome back to *Hacking Healthcare*.

Members of Parliament Levy New Charges against Huawei

Straight from our "Yes, This is Still a Thing" department, the latest twist in the long running Huawei saga comes to us via the United Kingdom (U.K.). A recent parliamentary inquiry has come out with numerous damaging conclusions that could pressure the U.K. government to remove Huawei from its 5G infrastructure even sooner than the 2027 deadline set earlier this year.[1] There are likely to be significant ramifications of the Parliament's inquiry regardless of whether its report leads to any concrete action on behalf of the U.K. government

We know you have plenty to pay attention to these days, so here is a quick reminder about what this is all about and why it matters. Huawei is a Chinese technology company that produces consumer electronics and telecommunications equipment, and it has grown rapidly over the years to be a major supplier of global 5G equipment. It has come under scrutiny recently by the United States government and some of its allies who accuse it of being funded by, and ultimately at the whim of, the Chinese government. Their concern is that integrating Huawei technology into next generation telecommunications networks represents a significant risk to national security by providing capabilities that could potentially enable cyber espionage or cyberattacks. This could include threats to critical infrastructure sectors such as healthcare.[2]

The most significant conclusion reached by the House of Commons Defense Committee is that Huawei is not nearly as independent from the Chinese Communist Party as they have repeatedly claimed. According to the "testimony of academics, cyber-security experts and telecom industry insiders," the Chinese government has financed Huawei's growth and Huawei has "engaged in a variety of intelligence, security, and intellectual property activities."[3, 4] The committee's recommendations based on these conclusions include accelerating the removal of Huawei telecommunications equipment by two full years and reconsidering Chinese investment in other critical sectors. For their part, Huawei has blasted the report for "[lacking] credibility as it is built on opinion rather than fact."[5]

Action & Analysis
H-ISAC Membership Required

CISA Releases Guidance on Ransomware and on Telework Essentials
On September 30th, CISA released both a comprehensive *Telework Essentials Toolkit* and a two-part *Ransomware Guide*. Both materials are freely available on CISA's website and are potentially valuable resources for organizations. Below, we break down what you can expect from each.

Ransomware Guide[6]

The *Ransomware Guide*, which is a joint venture with the Multi-State Information Sharing and Analysis Center (MS-ISAC), is 16 pages long and split into two parts. The first section, *Ransomware Prevention Best Practices*, informs readers of a number of ransomware infection vectors, general best practices, and hardening guidance. The second section, *Ransomware Response Checklist*, is a list of seventeen checkboxes for companies to consider, divided into categories of Detection & Analysis, Containment & Eradication, and Recovery & Post-incident Activity.

The guide's overview makes clear that it is "based on operational insight from [CISA] and [MS-ISAC]," and that its "audience… includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response."[7]

Telework Essentials Toolkit[8]

The Telework Essentials Toolkit is a short, 3-page infographic that dedicates each page to a different audience. The first page targets executive leaders and charges them with driving cybersecurity strategy, investment, and culture. The second page is for IT professionals who are tasked with developing security awareness and vigilance. The last page is aimed at teleworkers and those connecting via their home networks, and highlights raising security awareness. Each of these sections is filled out by several actions that the respective audience group should look to implement, as well as links to implementation tips and more comprehensive guidance.

Action & Analysis
H-ISAC Membership Required

Endpoint and IoT Security Check-up
A recent report on endpoint and IoT security released by Pulse Secure has helped to quantify the ways organizations in a broad swath of industries are coping with the growth of IoT and the transition of a significant percentage of their workforce to remote work. The results were

derived from 325 "IT decision-makers ranging from technical executives to IT security practitioners" from over 7 industries, including healthcare.[9] Participants' organizations ranged in size, but the majority were organizations of 5,000 or more employees, and all of the survey participants were based in the United States.[10]

Some of the more significant findings are:[11]

- 78% of participants said that IoT security is growing in importance as opposed to 3% who said it was becoming less important.
- At 78%, malware (ransomware, trojans, etc…) was the top endpoint and IoT device threat that participants were concerned about, with insecure network access / remote access ranking second at 61%, and compromised credentials in third with 58%.
- 39% of participants said the increase in remote work has significantly increased the amount of endpoint and IoT security issues they've seen.
- Loss of user productivity was the most significant impact of endpoint and security issues.
- Participants said the "high complexity of deployment and operation" was the biggest challenge to endpoint and IoT security.
- 56% of participants indicated it is at least moderately likely that they will be compromised by a cyberattack originating from endpoints or IoT devices.
- Increasing user awareness was the top near-term priority to reduce endpoint and IoT risk.

Action & Analysis
H-ISAC Membership Required

Survey:

Please take one minute to answer a few questions about this week's Hacking Healthcare by visiting this link: https://www.surveymonkey.com/r/VTCDYLP

Congress –

Tuesday, October 13th:
- No relevant hearings

Wednesday, October 14th:
- No relevant hearings

Thursday, October 15th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

Tuesday, October 20th:
- European Commission – Hearing – "The organisation of resilient health and social care following the COVID-19 pandemic"

Sundries –

Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work

https://krebsonsecurity.com/2020/10/amid-an-embarrassment-of-riches-ransom-gangs-increasingly-outsource-their-work/

US Ransomware Attacks Doubled in Q3; Healthcare Sector Most Targeted

https://healthitsecurity.com/news/us-ransomware-attacks-doubled-in-q3-healthcare-sector-most-targeted

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.bbc.com/news/technology-54455112

[2] https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSKCN1SR1EU

[3] https://www.bbc.com/news/technology-54455112

[4] https://www.theguardian.com/world/2020/oct/09/china-says-highly-concerned-about-safety-uk-investments

[5] https://www.bbc.com/news/technology-54455112

[6] https://www.cisa.gov/publication/ransomware-guide

[7] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

[8] https://us-cert.cisa.gov/ncas/current-activity/2020/09/30/cisa-releases-telework-essentials-toolkit

[9] https://www.pulsesecure.net/endpoint-iot-zero-trust/

[10] https://www.pulsesecure.net/endpoint-iot-zero-trust/

[11] https://www.pulsesecure.net/endpoint-iot-zero-trust/