November 10th, 2020

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* examines some new research on the behavior of consumers in different age demographics related to connected-device security habits and what it may mean for healthcare organizations deploying apps and wearables. Next, we briefly delve into a new report on how ransomware attacks with a data exfiltration element are becoming more common but also potentially less effective. Lastly, we provide a quick overview of new guidance on supply chain security for IoT that was published by the European Union Agency for Cybersecurity (ENISA). Welcome back to *Hacking Healthcare*.

1. Security Habits by Age Reveal Interesting Trends

In its *September 2020 Survey Report*, the National Cyber Security Alliance (NCSA) “engaged in a study to better understand consumer behavior around internet-connected devices and perceptions of security.”[1] Thie report also sought to examine what differences might exist between generations of American consumers. The results may not be completely surprising, but they do have implications for how healthcare sector organizations design products and services.

In a survey of 1,000 american citizens, split into two groups of 500 representing age brackets of 18-34 and 50-75, the survey asked numerous questions that related to internet-connected devices, privacy, and security.[2] Some of the more significant results were:[3]

- The younger demographic is significantly more likely than the older demographic to ‘always’ research a company’s data collection and user privacy policies at a 57% to 34% split

- The younger demographic is significantly more likely than the older demographic to use two-factor authentication at a 58% to 40% split

- The younger demographic is significantly more likely than the older demographic to check for software updates at 51% to 38% split

- The younger demographic is significantly more likely than the older demographic to be ‘very confident’ their connected devices are secure

- While the younger demographic is more likely to check on what information an app collects before downloading it, the older demographic tends to trust an app if it's from a reputable source
- Both demographics are more or less equal in their vigilance to change default passwords with the younger demographic leading 66% to 63%
- The older demographic was significantly more likely to make sure they always had an updated anti-virus or firewall at 49% to 33%
- For the healthcare sector, 74% of the younger demographic and 67% of the older demographic felt that telemedicine services were at least somewhat secure. However only 31% of total respondents felt they were 'very secure'

Action & Analysis
H-ISAC Membership Required

2. Ransomware Actors Reneging on Data Leaks

As many H-ISAC members will be well aware, the uptick in ransomware attacks has not spared the healthcare sector. Over the past many months, one of the strategic evolutions that has become more commonplace among ransomware incidents is the exfiltration of sensitive data from the victim's network. This exfiltrated data is often used as additional leverage to force a victim to pay a ransom by threatening the data's public release. A new report from Coveware sounds the not-so-surprising alarm that cybercriminals may no longer be holding up their end of the bargain to delete that data even after payment is made.[4]

In its Q3 report, Coveware states that "[a]lmost 50% of ransomware cases included the threat to release exfiltrated data along with encrypted data."[5] More distressingly, the report goes on to state that they have seen "a tipping point with the data exfiltration tactic," and a "fraying of promises of the cybercriminals to delete the data."[6] According to Coveware*, Sodinokibi*, *Maze*, *Netwalker*, *Mespinoza*, and *Conti* malware users have all gone back on their promises after being paid.[7] Coveware has seen evidence that victims were re-extorted weeks later with the same data, had their data publicly posted even after paying a ransom, or were given fake proof of data deletion.[8]

Action & Analysis
H-ISAC Membership Required

3. ENISA Releases Guidance for Securing the IoT Supply Chain

Securing the supply chain remains a hot cybersecurity topic for the private sector. For many industries, including healthcare, this already difficult task can become even harder when extended to emerging technology areas like IoT. Thankfully, ENISA has recently put forward comprehensive guidance for securing the IoT supply chain that organizations of all industry sectors can look to for assistance.

Released this week, ENISA's *Guidelines For Securing the Internet of Things: Secure supply chain for IoT* is a 52-page document that seeks to provide an overview of the IoT supply chain, threats to the IoT supply chain, 'good practices' for security, as well as more general guidance to improve IoT cybersecurity.[9] Meant for a varied audience that includes procurement teams, CISO's, IoT software developers and more, ENISA has attempted to include all stages of the IoT supply chain in its guidelines.

While there is great value in the entire document, ENISA concludes with 5 high level recommendations that are worth mentioning.[10]

1. **Forging Better Relationships Between Actors**: ENISA outlines how security issues can arise from poor communication and visibility between actors in the supply chain. They go on to list 'good practices' that can help mitigate potential communication issues as well as provide prominent international standards that organizations can look to for further guidance.
2. **Cybersecurity Expertise Should Be Further Cultivated**: ENISA supports maintaining a security aware workforce while also promoting risk-based approaches. Once again, ENISA lists applicable 'good practices' and international standards.
3. **Security by Design**: ENISA embraces the concept of security by design and then elaborates on various best practices that organizations should consider.
4. **Take A Comprehensive and Explicit Approach to Security**: ENISA states that most security threats detected along the IoT supply chain should be explicitly addressed. ENISA notes that proactively addressing issues is typically easier and less costly than trying to fix them afterwards.
5. **Leverage Existing Standards and Good Practices**: Finally, ENISA makes the case for adhering to existing, or developing new, IoT supply chain security standards through the collaboration of affected stakeholders.

Action & Analysis
H-ISAC Membership Required

U.S. Congress –

Tuesday, November 10th:
- No relevant hearings

Wednesday, November 11th:
- No relevant hearings

Thursday, November 12th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

- No relevant hearings

Sundries –

Suspected North Korean hackers who targeted job applicants prove more ambitious than first believed

https://www.cyberscoop.com/north-korean-hacking-lazarus-job-applicants/

US seizes more domains with ties to suspected Iranian influence campaign

https://www.cyberscoop.com/more-domains-seized-iran-doj/

Tech giants not convinced Australia's critical infrastructure Bill is currently fit for purpose

https://www.zdnet.com/article/tech-giants-not-convinced-australias-critical-infrastructure-bill-is-currently-fit-for-purpose/

Conferences, Webinars, and Summits –

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

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

[1] https://staysafeonline.org/wp-content/uploads/2020/11/NCSA_Cybersecurity-Awareness-Month-2020_Survey-Data-Report-1.pdf

[2] https://staysafeonline.org/wp-content/uploads/2020/11/NCSA_Cybersecurity-Awareness-Month-2020_Survey-Data-Report-1.pdf

[3] https://staysafeonline.org/wp-content/uploads/2020/11/NCSA_Cybersecurity-Awareness-Month-2020_Survey-Data-Report-1.pdf

[4] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[5] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[6] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[7] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[8] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[9] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[10] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things