October 23, 2018

TLP White

We start with an SEC investigative report examining a strain of cyber fraud. We also discuss the FDA's Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, as well as NIST's draft internal report regarding IoT cybersecurity and privacy risk mitigation. Speaking of IoT, we conclude by shedding some light on MQTT flaws which have a substantial impact on IoT devices.

Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***SEC Report Issues Warning Shot.*** A new Securities and Exchange Commission ("SEC") investigative report urges companies to consider cyber threats when implementing internal accounting controls to mitigate the risk of business email compromises ("BEC"), a common form of cybersecurity fraud.[1] This type of cybersecurity fraud involves an unauthorized individual posing as company executives or vendors and using emails to trick company employees into sending large sums of money to bank accounts that are under the control of the unauthorized person.

   Where a company lacks sufficient monitoring capabilities, BECs can be carried out over a period of months while remaining undetected. The financial impact of this fraudulent cyber scheme can be severe. The SEC's investigative report examines nine public companies that lost a combined total of almost $100 million dollars as a result of BECs.[2] Moreover, the FBI estimates that fraud involving BECs has cost companies more than $5 billion since 2013.

   The SEC's investigative report recommends that companies devise and maintain internal accounting controls that reasonably safeguard company (and therefore investor) assets from cyber-related frauds.[3] This recommendation stems from the obligations set forth in the Securities and Exchange Act, which requires covered entities to "devise and maintain a system of internal accounting controls sufficient to provide reasonable

[1] https://www.sec.gov/litigation/investreport/34-84429.pdf
[2] https://www.sec.gov/news/press-release/2018-236
[3] https://www.sec.gov/litigation/investreport/34-84429.pdf

assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization."[4]

2. ***To Fail to Plan is to Plan to Fail.*** The Food and Drug Administration ("FDA") has recently released several guidance documents addressing the security of medical devices, a particular area of focus for the agency. This month, the MITRE Corporation, on behalf of the FDA, released the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. The playbook was created to help facilitate communication among healthcare delivery organizations ("HDO") and other stakeholders in the event of a medical device cybersecurity incident.

   The purpose of the playbook is "to serve as a tool for regional readiness and response activities to aid HDOs in addressing cybersecurity threats affecting medical devices that could impact continuity of clinical operations for patient care and patient safety."[5] The framework provided in the guidance was designed to help establish roles and responsibilities among those who may be tasked with responding to a cyber incident within a healthcare delivery organization before a medical device cybersecurity incident occurs. It also seeks to facilitate communication between and improve coordination among healthcare delivery organizations as well as with government (local, state, and federal). The playbook is stakeholder-derived, open source, and customizable, designed to give HDOs flexibility in how they choose to leverage the framework depending on the organization's specific needs so that it is as least disruptive as possible to patient care and wellbeing.

   MITRE invites stakeholders to provide feedback and comments on the playbook via email at securemed@mitre.org.

3. ***NIST Seeks Comments on IoT Risk Mitigation Report.*** Last week, the National Institute of Standards and Technology ("NIST") released draft NIST Internal Report (NISTIR") 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks for public comment. NIST created the NISTIR to help organizations address cybersecurity and privacy threats that impact IoT devices throughout the device lifecycle. Specifically, the NISTIR identifies high-level considerations that may impact IoT cybersecurity and privacy risk management, as distinguished from other, non-IoT devices.[6] The document also provides recommendations for organizations regarding how to address risk considerations impacting their IoT devices.

   The NISTIR was designed to help federal agencies as well as other organizations understand and manage relevant cybersecurity and privacy risks posed by IoT devices.

---

[4] 15 U.S.C. § 78m.

[5] https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf

[6] https://www.nist.gov/blogs/i-think-therefore-iam/dont-leave-us-our-own-devices-seeking-feedback-draft-nistir-iot

To that end, NIST is soliciting feedback on the NISTIR to help the agency understand: (1) the efficacy of the NISTIR's distinctions between conventional IT and IoT; (2) whether the distinctions that have been drawn in this context are reasonable as compared to how risk response is addressed in other contexts; and (3) moving forward, which aspects of managing cybersecurity and privacy risks for IoT devices NIST should address.

NIST is soliciting feedback on the NISTIR through October 24, 2018. Additional details regarding comment submission can be found here.

4. ***Researchers to Present on Substantial MQTT Flaws.*** Two security researchers are slated to present during Black Hat Europe regarding troves of data that they were able to collect from hundreds of thousands of Message Queuing Telemetry Transport ("MQTT") servers.[7] This data was located on sensors and other devices that were in manufacturing and automotive networks, in addition to consumer Internet of Things ("IoT") devices.

   One of the researchers collecting the data reported that the MQTT servers that he found were open to the public Internet via Shodan, and noted that he would probe and listen to the servers for 10 or so seconds, collecting data from them. Once the two researchers, which had been separately collecting data from the MQTT servers, combined forces they were able to better understand how MQTT and another protocol, the Constrained Application Protocol ("CoAP") could be abused by bad actors. The researchers determined that widely used device-to-device communications protocols contained inherent security weaknesses, particularly with respect to their implementation on IoT devices. These security weaknesses expose flaws that could permit bad actors to execute denial-of-service attacks or gain remote control of industrial or consumer IoT devices for any number of nefarious activities, including cyber espionage. Furthermore, these flaws can permit a bad actor to leverage compromised IoT devices to move laterally on the network that the compromised device is connected to.

   Further complicating the matter, the MQTT protocol standard has been evolving over the last few years. As a result, older versions may be left without critical security fixes.

Congress –

Tuesday, October 23:
--No relevant hearings.

Wednesday, October 24:
--No relevant hearings.

[7] https://www.darkreading.com/vulnerabilities---threats/new-security-woes-for-popular-iot-protocols/d/d-id/1333069?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple

Thursday, October 25:
--No relevant hearings.

International Hearings/Meetings –

EU –

Tuesday, November 13:
--Hearing entitled, "Assessing the impact of digital transformation of health services" (EU Commission's Expert Panel on Health).[8]

Conferences, Webinars, and Summits –

--Summit on Third-Party Risk – Leesburg, VA (10/24-26) <https://nhisac.org/events/nhisac-events/summit-on-third-party-risk/>
--2018 Healthcare CyberGard Conference – Charlotte, NC (10/25-26)
https://nhisac.org/events/nhisac-events/2018-heathcare-cybergard-conference/
--H-ISAC Radio member-to-member discussion on Software Bill of Materials – 10-29 Noon ET; link will be sent in member listerver.
--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>
--FIRST Symposium 2019 – London, UK (3/18/19)
<https://nhisac.org/events/nhisac-events/first-symposium-2019/>
--2019 NH-ISAC Spring Summit – Ponte Vedra Beach, FL (5/13-17)
<https://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>

Sundries –

--**The key to protecting the midterms is resilience for election systems, experts say**
<https://www.cyberscoop.com/chris-krebs-robby-mook-matt-masterson-cybertalks/>
--**Takeaways from Twitter's data trove**
<https://www.politico.com/newsletters/morning-tech/2018/10/18/takeaways-from-twitters-data-trove-378432>
--**Apple's New Data & Privacy Portal Lets You Download Your Data**
<https://www.bleepingcomputer.com/news/apple/apples-new-data-and-privacy-portal-lets-you-download-your-data/>

[8] https://ec.europa.eu/health/expert_panel/events_en

October 23, 2018

--**Researcher Livestreams 51% Attack on Altcoin Blockchain**
<https://www.bleepingcomputer.com/news/security/researcher-livestreams-51-percent-attack-on-altcoin-blockchain/>
--**Industry groups sue Vermont over state's net neutrality rules**
<https://thehill.com/policy/technology/412120-industry-groups-sue-vermont-over-states-net-neutrality-rules>
--**Inside the Dark Web's 'Help Wanted' Ads**
<https://www.darkreading.com/threat-intelligence/inside-the-dark-webs-help-wanted-ads/d/d-id/1333066?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple>
--**Former Equifax Manager Sentenced for Insider Trading**
<https://www.darkreading.com/attacks-breaches/former-equifax-manager-sentenced-for-insider-trading/d/d-id/1333070?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple>

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