September 22nd, 2020

TLP White

This week, *Hacking Healthcare* begins by examining the sobering news that ransomware has been cited as likely being responsible for an individual's death. Next, we highlight some recent work conducted by the National Institute of Standards and Technology (NIST) that has resulted in a new tool to help organizations fight phishing. Lastly, we brief you on the benefits of the United States Cybersecurity and Infrastructure Security Agency's (CISA) integration into the CVE process. ***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*.

1. **Ransomware Investigated as Primary Cause of Death.** Last week, a woman in Düsseldorf, Germany, was reportedly unable to receive urgent medical attention after the hospital she was scheduled to receive treatment at was is the midst of a ransomware attack.[1] During her resulting 19 mile journey to another hospital, the woman reportedly passed away.[2] According to the former chief executive of the UK's National Cyber Security Centre, Ciaran Martin, "[i]f confirmed, this tragedy would be the first known case of a death directly linked to a cyber-attack."[3]

   On the evening of September 9th, Düsseldorf University Hospital was apparently hit by ransomware that took essential systems offline and impacted 30 internal servers.[4] The infection was allegedly the result of cybercriminals making use of "a vulnerability in a widely used commercial [VPN] software."[5] Current reports suggest that BSI, the Federal Office for Information Security, is now on-site "helping the hospital's IT staff rebuild systems," while authorities investigate the link between the ransomware attack and the cause of death.[6]

   According to reporting from ZDNet, "[i]f the ransomware attack and the hospital downtime are found to have been directly at fault for the woman's death, German police said it plans to turn their investigation into a murder case."[7]

   Action & Analysis
   H-ISAC Membership Required

2. **NIST Goes Phishing**. As we've previously reported, the transition to remote work as a result of COVID-19 predictably led to a surge in malicious cyber activity. In particular,

phishing has been one of the major threat techniques that saw a massive increase in use over the past six months, and it is one that continues to present a considerable threat to organizations. Malicious actors making use of phishing have been preying on individuals' fears and curiosity over COVID-19 in order to incentivize ill-advised clicks onto malicious links and emails.

Fortunately, there may be a new tool to help combat this threat. On Thursday, September 17th, NIST issued a press release detailing their development of "a new method called the Phish Scale that could help organizations better train their employees to avoid a particularly dangerous form of cyberattack known as phishing."[8]

In the press release, NIST recognized that while many organizations often have some level of phishing awareness programs in place, these programs typically rely on simplistic metrics to measure success, such as clicked views. Without an accurate way to measure the effectiveness of an organization's phishing awareness and defense program, it can be difficult to know how well a workforce is doing.

NIST's tool aims to solve that problem. The "Phish Scale is intended to help provide a deeper understanding of whether a particular phishing email is harder or easier for a particular target audience to detect." The tool proposes a rating system on a five-point scale and is based on the "scenario's premise," which should help security professionals better understand how difficult it is for employees to discern that an email was malicious.

NIST's next steps with the Phish Scale include "[expanding] the [data] pool and [acquiring] data from other organizations, including nongovernmental ones, and to make sure the Phish Scale performs as it should over time and in different operational settings."[9]

Action & Analysis

H-ISAC Membership Required

3. **CISA Integrates into CVE Process for Medical Devices**. Last week, it was reported that CISA would take over responsibility for assigning Common Vulnerability Enumeration (CVE) identifiers for medical devices and industrial control systems (ICS).[10] This planned move makes CISA the first peer organization to MITRE, which oversees the CVE process.

   On September 15th, MITRE, the non-profit organization that manages the CVE program, released a statement that CISA was expanding its partnership with MITRE to become a "Top-Level Root CVE Numbering Authority for industrial control systems (ICS) and medical device vendors participating as CVE Numbering Authorities (CNAs)."[11] As a Top-level Root CNA, CISA will be tasked with managing CNA's within ICS and medical devices. Their responsibilities will now include "ensuring the effective assignment of CVE IDs, implementing the CVE Program rules and guidelines, and managing the CNAs under its

care."[12] Furthermore CISA will be "responsible for recruitment and onboarding of new CNAs and resolving disputes within its scope."[13]

For its part, CISA stated that they hope this expansion of their partnership will "encourage more vendors to participate in the CVE program and allow CISA to better support stakeholders as they become more engaged."[14] They also cited how "public and transparent disclosure of industrial control systems and medical device vulnerabilities is a critical mission for CISA."[15]

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/2G5DB9C

Congress –

Tuesday, September 22nd:
- Senate – Committee on Homeland Security and Governmental Affairs - Subcommittee on Federal Spending Oversight and Emergency Management: Hearings to examine state and local cybersecurity, focusing on defending communities from cyber threats amid COVID-19.

Wednesday, September 23rd:
- Senate - Committee on Commerce, Science, and Transportation: Hearings to examine the need for federal data privacy legislation.
- Senate – Committee on the Judiciary- Subcommittee on Intellectual Property: Hearings to examine threats to American intellectual property, focusing on cyber-attacks and counterfeits during the COVID-19 pandemic.
- House - Committee on Science, Space, and Technology: Subcommittee on Investigations and Oversight - Hearing: "Data for Decision-Making: Responsible Management of Data during COVID-19 and Beyond"

Thursday, September 24th:
- Senate – Committee on Commerce, Science, and Transportation - Subcommittee on Communications, Technology, Innovation, and the Internet: Hearings to examine an evaluation of FirstNet's progress.

International Hearings/Meetings –

- No relevant hearings

EU –

Tuesday, September 22nd:
European Parliament – Committee on Environment, Public Health, Food Safety

September 22nd, 2020

Sundries –

Patients want to download their own health data, report shows

https://www.healthcareitnews.com/news/patients-want-download-their-own-health-data-report-shows

FBI hopes a more aggressive cyber strategy will disrupt foreign hackers

https://www.cyberscoop.com/fbi-cyber-strategy-hackers-tonya-ugoretz/

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-54204356
[2] https://www.bbc.com/news/technology-54204356
[3] https://www.bbc.com/news/technology-54204356
[4] https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/
[5] https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/
[6] https://www.bbc.com/news/technology-54204356
[7] https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/
[8] https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click
[9] https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click
[10] https://www.darkreading.com/vulnerabilities---threats/vulnerability-management/cisa-joins-mitre-to-issue-vulnerability-identifiers/d/d-id/1338930
[11] https://cve.mitre.org/news/press_release/CVE_Program_Partners_with_Cybersecurity_Infrastructure_Security_Agency_to_Protect_Industrial_Control_Systems_and_Medical_Devices.html
[12] https://cve.mitre.org/news/press_release/CVE_Program_Partners_with_Cybersecurity_Infrastructure_Security_Agency_to_Protect_Industrial_Control_Systems_and_Medical_Devices.html
[13] https://cve.mitre.org/news/press_release/CVE_Program_Partners_with_Cybersecurity_Infrastructure_Security_Agency_to_Protect_Industrial_Control_Systems_and_Medical_Devices.html
[14] https://www.cisa.gov/news/2020/09/15/cisa-oversee-cve-numbering-authorities-industrial-control-systems-and-medical
[15] https://www.cisa.gov/news/2020/09/15/cisa-oversee-cve-numbering-authorities-industrial-control-systems-and-medical