October 29nd, 2019

TLP White

In this edition of Hacking Healthcare, we breakdown the United Kingdom's National Cyber Security Centre's annual review. Next, we examine the U.S. Department of Homeland Security's push for U.S. federal agencies to implement vulnerability disclosure programs. Finally, we lament the discovery of another set of unsecured medical databases and what you should do when it comes to securing sensitive data in the cloud. Welcome back to *Hacking Healthcare*.

1. **The United Kingdom's Cyber Centre Publishes its Yearly Review.** From our "Who Doesn't Love Free Stuff" department, we bring you the NCSC's annual report. In 2016, the government of the United Kingdom (U.K.) created the National Cyber Security Centre (NCSC). The Centre, which operates in a similar role to the United States' Cybersecurity and Infrastructure Security Agency (CISA), describes its role as "[supporting] the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public," and "providing effective incident response [and recovery]".[1] Last week, the NCSC released its 2019 Annual Review. The 94-page report is broken down into numerous sections focusing on the various sectors the NCSC helps to secure and the key issues with which they are engaged. The following summarizes those sections and the key takeaways of each.

   The report opened with a high-level statistical assessment of the work and achievements they were involved in over the past year. These included handling 658 incidents, supporting nearly 900 victim organizations, producing 154 threat assessments and 34 pieces of guidance, and enabling numerous events and programs focused on education and outreach.[2] The full list of highlighted statistics helps to underscore the comprehensiveness of the NCSC's capabilities.

   The following section on cybersecurity for individuals and families makes clear that education and awareness are still the top priorities when it comes to the general public. This is illustrated by their emphasis on password management, multi-factor authentication, and patch/update installation, while also calling attention to the NCSC's work on promoting 'Secure by Design' principles in everyday products.

   The next section detailed the NCSC's Active Cyber Defense program, critical infrastructure protection, regulation, and national security developments. No section

better details the sheer breadth of cyber related activities that require active NCSC involvement. Everything from securing critical infrastructure, engaging with international standards and implementing new regulations, to supporting armed forces weapons development and securing industry supply chains is included.

The subsequent section on countering the adversary outlined the NCSC's commitment to intelligence gathering of threats and informing strategic responses, incidence response and management, and their role in advising on policy matters. The highlight of the section was the NCSC's introduction of the Cyber Defence Ecosystem (CDE). The CDE is meant to be a more structured, resourced, and improved version of threat analysis and information sharing that is country-wide and utilizes automation to speed associated processes.

The final two sections focused on securing the digital homeland and looking to the future with the common themes of education and awareness. The NCSC has made significant investments in creating and advertising their online presence, providing toolkits for business that allow them to assess their resilience and to better prepare their board of directors, and partnering with schools to provide cyber training. However, the most significant program the NCSC highlighted was their CyberFirst initiative, which "aims to identify and nurture young talent, engaging students from all backgrounds and regions, helping them to explore their passion for technology and providing them with the necessary skills and knowledge to put it into practice."[3] The initiative creates a pathway for individuals as young as 11 to begin training to fill the United Kingdom's ranks of cyber professionals.

This report is well worth the read, regardless of whether you are a UK based organization or not, and regardless of sector and we recommend that your security teams keep an eye on everything the NCSC produces; they are valuable resources that will supplement everything you do in your cybersecurity program.

2. **DHS Pushes for Federal Vulnerability Disclosure Programs.** The Department of Homeland Security (DHS) is considering the possibility of issuing a Binding Operational Directive (BOD) that would require civilian agencies within the federal government to stand up vulnerability disclosure programs (VDPs). The impetus for the potential BOD is the unsatisfactory rate at which federal agencies are implementing VDPs. Despite the months of work that have gone into the planning for the issuance of a BOD, there are reports that DHS would like to find other incentives if possible.[4]

   The reluctance that some federal agencies feel towards adopting a VDP is understandable; some view it as incentivizing outsiders to attack their systems which puts stress on already overworked security teams. Other rationalizations include the notion that you know your system and products better than anyone else could, so

spending time investigating outside reports is likely to be a waste, or that a deluge of disclosed vulnerabilities could be impossible to remediate within the given timeline.

Regardless of the trepidation that may come with implementing a VDP, the importance and benefits of VDPs cannot be overstated. Providing that a clear process by which vulnerabilities can be reported, the necessary information needed for remediation is outlined, and the likely timeline for that remediation is stated, will help to ensure that all parties avoid misunderstandings stemming from misaligned expectations and assumptions. VDPs are widely lauded within both the private and public sector, and the H-ISAC encourages organizations to explore the many readily available resources on VDP implementation if you don't already have one in place. The H-ISAC is happy to assist if you need further guidance.

3. **Do You Know Where Your Data Is?** Another week, another group of unsecured databases leaking sensitive information to anyone who comes across them. Last week's findings from two research groups were particularly egregious as they contained sensitive patient information and personal information of United States government and military personnel. Additionally, as if discovering the unsecured databases wasn't bad enough, the researchers had great difficulty in contacting the necessary parties involved to get the databases secured, with some still unsecured at the time they finally publicly released their findings.[5]

   First, the security team from WizCase announced that they had discovered nine unsecured medical databases from numerous organizations based in Europe, North America, South America, Asia, and Africa. The databases, which potentially impacted millions of individuals, allegedly contained everything from the results of lab visits and prescriptions to names and social security numbers.[6] WizCase claims that a ransom note was among the files they analyzed, which could imply that that malicious actors had already found and potentially exfiltrated sensitive patient data.[7]

   The second incident involved an unsecured database belonging to Autoclerk, which is a service owned by the Best Western Hotels and Resorts group.[8] According to vpnMentor, the company who found the unsecured database, 179GB worth of data impacting thousands of individuals' sensitive information was freely available to anyone who happened to come across the database.[9] Among the included information were names, dates, phone numbers, and addresses, although credit card details appear to have been spared.[10] However, a further unwelcome surprise was the revelation that members of the U.S. government and military were also affected. Autoclerk appears to have been connected to a government contractor that oversees travel arrangements, this ended up exposing both past and future travel details of members of the U.S. government and military.

October 29nd, 2019

Congress –

Tuesday, October 29th:
- No relevant hearings

Wednesday, October 30th:
- No relevant hearings

Thursday, October 31st:
- Hearings to examine supply chain security, global competitiveness, and 5G (Senate Committee on Homeland Security and Governmental Affairs)

International Hearings/Meetings –

EU –

-No relevant hearings

Conferences, Webinars, and Summits –

--H-ISAC Security Workshop – Titusville, FL (11/4/2019)
https://h-isac.org/hisacevents/h-isac-security-workshop/
--Maximize your Threat Sharing by Anomali – Webcast (11/6/2019)
https://h-isac.org/hisacevents/maximize-your-threat-sharing/
--CHIME Healthcare CIO Boot Camp – Phoenix, AZ (11/6/2019-11/9/2019)
https://h-isac.org/hisacevents/chime-healthcare-cio-boot-camp/
--Health IT Summit (Southwest) – Houston, TX (11/14/2019-11/15/2019)
https://endeavor.swoogo.com/2019-Dallas-Health-IT-Summit
--Southwest Healthcare Cybersecurity Forum – Dallas, TX(11/15/2019)
https://endeavor.swoogo.com/2019_Southwest_Cybersecurity_Forum
--Health IT Summit (Northwest) – Seattle, WA (11/19/2019-11/20/2019)
https://endeavor.swoogo.com/2019-PacificNorthwest-HITSummit
--Pacific Northwest Healthcare Cybersecurity Forum – Seattle, WA (11/20/2019)
https://endeavor.swoogo.com/2019_Pacific_Northwest_Cybersecurity_Forum
Cyber Security & Data Protection Summit 2019 – London, UK (11/20/2019)
https://cybersecuritysummit.co.uk/
--2019 H-ISAC Fall Summit – San Diego, CA (12/2/19-12/6/2019)
https://h-isac.org/summits/fall-summit-2019/
--H-ISAC Security Workshop – London, UK (2/5/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-2/
-- H-ISAC Security Workshop - Cambridge, MA (4/7/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-cambridge-ma/

Sundries –

--Military Algorithm Can Predict Illness 48 Hours Before Symptoms Show
https://www.nextgov.com/analytics-data/2019/10/military-algorithm-can-predict-illness-48-hours-symptoms-show/160851/

October 29nd, 2019

--Rise in Stalkerware: The software that spies on your partner
https://www.bbc.com/news/technology-50166147
--Why One Secure Platform Passed on Two-Factor Authentication
https://www.wired.com/story/keybase-two-factor-authentication/
--NordVPN admits 'isolated' data breach was discovered last year
https://www.cyberscoop.com/nordvpn-data-breach/

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

[1] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
[2] https://www.ncsc.gov.uk/annual-review/2019/ncsc/docs/ncsc_2019-annual-review.pdf
[3] https://www.ncsc.gov.uk/annual-review/2019/ncsc/docs/ncsc_2019-annual-review.pdf
[4] https://www.cyberscoop.com/dhs-vulnerability-disclosure-program-bod/
[5] https://healthitsecurity.com/news/9-unsecured-medical-databases-found-leaking-sensitive-patient-data
[6] https://www.wizcase.com/blog/medical-breaches-research/
[7] https://www.wizcase.com/blog/medical-breaches-research/
[8] https://www.zdnet.com/article/autoclerk-database-leaked-customer-government-and-military-personal-records/
[9] https://www.zdnet.com/article/autoclerk-database-leaked-customer-government-and-military-personal-records/
[10] https://www.zdnet.com/article/autoclerk-database-leaked-customer-government-and-military-personal-records/