February 25th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by highlighting a new report that suggests healthcare organizations may not always appreciate the cybersecurity risks related to their relationships with third-party business associates. Then, we briefly examine how France has cited cyberattacks against its hospitals as an impetus for a new €1 billion initiative to improve its overall cybersecurity ecosystem. Welcome back to *Hacking Healthcare*.

1. New Report Highlights Third-Party Risks to Health Organizations

Healthcare sector organizations, just like entities in other sectors, rely heavily on a wide range of third-party business associates to efficiently and cost-effectively address their numerous business needs. Unfortunately, even for organizations that have the resources and expertise to implement cybersecurity best practices themselves, third-party business associates can introduce hard-to-manage risks. As a new report from CI Security highlights, healthcare organizations may increasingly be targeted for cyberattacks through their connections to and reliance on third-party business associates.

CI Security released its *2020 Healthcare Data Breach Report* this month. The publication reported that healthcare data breaches increased in the second half of the year, and that "nearly three-quarters of all breaches [were] tied to third parties."[1] CI Security noted that this reported increase was not necessarily unsurprising, as the initial challenges of responding to COVID-19 impacted security practices and investigative resources. However, the authors were 'alarmed' at "the apparent shift in tactics among cybercriminals, who have evolved their methods to attack the soft underbelly of healthcare networks – third party business associates."[2]

The report goes on to note the wide variety of services that were compromised, including billing, insurance reimbursement, and fundraising software. CI Security attributes at least part of this shift to the likelihood that third-party business associates are less secure, but also because they have the potential to infect multiple targets and may be willing to pay a larger ransom themselves.[3]

Action & Analysis
H-ISAC Membership Required

2. **French Hospital Cyberattacks Help Spur IT Investment**

Attacks against the healthcare sector in recent months have not gone unnoticed by the French government. Last week, French President Emmanuel Macron signaled his intent to bolster cybersecurity preparedness in his country by investing "€1 billion in a national cybersecurity strategy."[4] The urgency for the move was allegedly reinforced by the recent cyberattacks against hospitals in Dax and Villefranche-sur-Saône.[5]

The two hospitals were reportedly hit by ransomware that "affected patient records, surgical devices, medication management, appointments, [and] bed and doctor allocation," and forced patient operations to be postponed.[6] Despite assistance from France's National Information Systems Security Agency (ANSSI), a return to normal operation is not expected for several weeks.[7] Macron reportedly referenced the attacks as proof of needed investment in France's overall cybersecurity.

It isn't completely clear how that €1 billion will be spent, but early reports suggest that "€500 million [will be spent] to fund research and help companies improve their technologies and develop more robust cyber defence systems."[8] Unconfirmed reports suggest that €350 million will be dedicated to hospitals.[9] Additional support in this area will also likely come from a new cybersecurity center opening in Paris that will support 1,500 individuals from public and private sector entities.

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, February 23rd:
- No relevant hearings

Wednesday, February 24th:
- No relevant hearings

Thursday, February 25th:
- House of Representatives: Committee on Appropriations – Subcommittee on the Departments of Labor, Health and Human Services, Education, and Related Agencies: *Ready or Not: U.S. Public Health Infrastructure*

International Hearings/Meetings –

- No relevant hearings

EU –

Thursday, February 25th:
- European Parliament – Committee on the Environment Public Health and Food Safety: *A reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices*

February 25th, 2021

Conferences, Webinars, and Summits –
https://h-isac.org/events/

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

[1] https://www.healthcareitnews.com/news/business-associates-were-largely-blame-2020-breaches

[2] *2020 Healthcare Data Breach Report: An Analysis of HHS Breach Reports in 2020*. Critical Insight by Critical Security. 2021

[3] *2020 Healthcare Data Breach Report: An Analysis of HHS Breach Reports in 2020*. Critical Insight by Critical Security. 2021

[4] https://www.healthcareitnews.com/news/emea/emmanuel-macron-pledges-1bn-cybersecurity-after-hospital-ransomware-attacks

[5] https://www.healthcareitnews.com/news/emea/emmanuel-macron-pledges-1bn-cybersecurity-after-hospital-ransomware-attacks

[6] https://www.healthcareitnews.com/news/emea/emmanuel-macron-pledges-1bn-cybersecurity-after-hospital-ransomware-attacks

[7] https://www.healthcareitnews.com/news/emea/emmanuel-macron-pledges-1bn-cybersecurity-after-hospital-ransomware-attacks

[8] https://www.thelocal.fr/20210219/macron-announces-1bn-security-package-after-cyberattacks-on-french-hospitals

[9] https://www.hstoday.us/subject-matter-areas/cybersecurity/france-invests-e350-million-for-hospital-cybersecurity-after-attacks-increase/