WILLIAMS MULLEN
WILLIAMSMULLEN.COM

Health Care Industry Still a Prime Target for Ransomware Attacks - Don't Let Them Make You WannaCry

06.26.2017

The global ransomware attack known as “WannaCry” was among the biggest news stories in May, bringing the term “ransomware” into widespread public awareness. For more information on the “WannaCry” ransomware attack, see Williams Mullen’s recent alert here. Despite the relative novelty of the magnitude of the attack, the health care industry consistently has been a target of these types of attacks, and the recent WannaCry virus should serve as a reminder to health care providers and others in the industry that the threat will not abate anytime soon.

Among those hardest hit in the “WannaCry” attack was the British National Health Service (NHS), which had 16 hospitals critically impacted by the virus. The NHS was forced to reschedule patient appointments and procedures and divert patients from affected centers.[i] Although the U.S. health care system was not as hard hit as the NHS and other companies in other industries worldwide, it did not escape unscathed. The Department of Health and Human Services (HHS) issued a notice on June 6, 2017, that two American health systems still were working towards normal system operations after being attacked by WannaCry, and *Forbes* reported that there were a small number of instances of medical devices being locked down by the WannaCry virus.[ii]

As stated above, this is not the first time that the health care sector has made the news for ransomware attacks. In 2016, one of the most high-profile attacks was perpetrated against Hollywood Presbyterian Medical Center in California. Held hostage for a bitcoin equivalent of less than $20,000, Hollywood Presbyterian experienced massive disruptions in services. Its computers were down for more than a week before the system was restored, preventing them from accessing key documentation, including radiology, pharmacy, and laboratory records, and forcing the hospital to divert patients.[iii] Although hospitals and health systems are common victims of these cyberattacks, physician practices and clinics also have experienced their own problems with ransomware.[iv]

These viruses have become a persistent threat, and HHS has published several guidance documents in its effort to assist the health care sector prepare for, respond to, and mitigate the effects of ransomware attacks. In 2016, HHS promoted a report issued by multiple federal agencies on identifying and responding to ransomware attacks.[v] In addition, the Office for Civil Rights at HHS published guidance detailing how ransomware attacks interplay with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and covered entities’ and business associates’ responsibilities for Security Rule and breach notification compliance.[vi]

Most recently, HHS issued several updates to its listserv subscribers as the WannaCry virus and its aftermath unfolded. These updates contained advice on how to avoid ransomware attacks and who to contact in the event of a ransomware attack. HHS linked readers to Microsoft's security websites and other federal government resources on cybersecurity reporting and preparation.

The Health Care Industry Cybersecurity Task Force recently issued a report stating that "the rise and sophistication of ransomware attacks that hold IT systems and patient-critical devices hostage continues to grow, as evidenced by hospital ransomware attacks of 2016." The report concluded that "health care cybersecurity is a key public health concern that needs immediate and aggressive attention."[vii] Health care providers and other organizations in the health care industry need to provide the "immediate and aggressive attention" that the ransomware threat requires.

[i] L. Smith-Spark, et al., "NHS: No evidence of patient data breach in cyberattack," *CNN* (May 13, 2017), available at http://www.cnn.com/2017/05/13/health/uk-nhs-cyber-attack/index.html.

[ii] E. Sweeny, "HHS: Two large healthcare systems still face 'significant' operational challenges from WannaCry," *FierceHealthcare.com* (Jun. 6, 2017), available at http://www.fiercehealthcare.com/privacy-security/hhs-two-large-healthcare-systems-are-still-dealing-wannacry; T. Fox-Brewster, "Medical Devices Hit by Ransomware for the First Time in US Hospitals," *Forbes* (May 17, 2017), available at https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#401d86fe425c.

[iii] S. Ragan, "Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers," available at http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html.

[iv] E. Dietsche, "12 healthcare ransomware attacks of 2016," *Becker's Health IT & CIO Review,* (Dec. 29, 2016), available at http://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html.

[v] “How to Protect Your Networks from Ransomware,” available at https://www.justice.gov/criminal-ccips/file/872771/download.

[vi] “Fact Sheet: Ransomware and HIPAA,” available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

[vii] “Report on Improving Cybersecurity in the Health Care Industry,” (June 2017), available at https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

Related People