SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog October 2020

Topics covered in this issue:

- Ransomware and malware attacks on U.S. hospitals

https://www.wwnytv.com/2020/07/28/western-ny-hospital-recounts-ransomware-experience-smc-deals-with-malware-attack/

The first article in this resource list is an article from a local news station which pertains to a malware attack on a hospital. According to the article, the hospital, Samaritan Medical Center in western New York, was unable to access their proprietary computer network and data, and as of the writing of the article (July 28th, 2020) had still not regained access. The article confirms that an investigation into the source of the outage was malware, and indicates that the hospital had reverted to using pen and paper. An article appearing on the website Cyberscoop written by Sean Lyngaas on August 20th (https://www.cyberscoop.com/samaritan-medical-center-new-york-malware-recovery/) indicates that the hospital had been able to regain access to patient's medical records as well as accounting data, but that full network access was still elusive.

The first article draws parallels between this recent attack on Samaritan Medical Center and a ransomware attack on a similar healthcare facility in nearby Buffalo, New York in 2017 (this incident was explored in detail in a previous report by this author for Ward Sciences and Consulting, LLC). In the case of the Buffalo healthcare facility (the Erie County Medical Center), several desktop computers on the facility's network began displaying messages demanding hundreds of thousands of dollars in cryptocurrency in exchange for renewed access to patient records. In the case of the Erie County Medical Center, the decision was made not to pay the ransom and instead to utilize their backup system and of records and to rebuild the computer system - a process greatly aided by the $10 million dollar insurance policy they had purchased just a few months prior to protect them against cybersecurity threats.

The story of the Erie County Medical Center brings attention to a number of interesting dimensions as it pertains to cybersecurity, particularly ransomware, within the critical infrastructure of healthcare, and many other critical infrastructures which are vulnerable.

John Ward – Cyberblog October 2020

As these two incidents, as well as countless other in recent history, make clear, ransomware attacks are becoming increasingly popular and are on the rise (previous reports in this series by this author have highlighted the proliferation of ransomware-for-hire providers, as well as the low technological capabilities, both in terms of hardware and knowledge, that a perpetrator needs to successfully perform a ransomware attack. As the articles above point out, the Erie County Medical Center was prepared for a cyberattack, as they had sufficiently backed up their records and had an insurance plan in place for just such an occasion. The articles above do not mention if the Samaritan Medical Center had any such preventative/recovery measures in place. Even with the measures taken by the Erie County Medical Center, they were still off-line for a significant period of time, which in the healthcare industry can mean the difference between life and death. There is no telling how much of an effect and the duration of a ransomware attack on a healthcare facility with less mitigating factors could have, and the Samaritan Medical Center could be window into just how much damage can be done.

It is important to note that in both cases, the facilities did not pay the ransom. This is an important piece of information as it indicates that, at least in the healthcare community, there are a significant number of decision-makers and administrators who are choosing not to pay. This is an important development; meeting the perpetrator's demands financially has no guarantee that they will uphold their end of the bargain, and thus an affected entity could be without access in addition to being out a significant amount of money. Furthermore, payment of a ransom could set a dangerous precedent, and mark an entity as an easy target Non-payment of ransomware ransom has been an ever-more attractive option for affected entities as the ransomware threat develops-the April report in this series by this author explored a bill before the New York legislature, the region of the country where both Samaritan Medical Center and the Erie County Medical Center are located, which would prohibit the use of municipal funds to meet the financial demands of those employing ransomware. As it seems to be an unfortunate certainty that similar ransomware attacks will continue to proliferate, it is important to monitor how they are responded to, both from a single-entity and a collective perspective. This is not a problem that will be going away, and the actions of individual affected entities, collective industries (especially critical infrastructure), and legislators will play a large part in shaping deterrence and response as the threat evolves.