SEISENSE Journal of Management
Vol 1 No 4 (2018): DOI: https://doi.org/10.5281/zenodo.1435408, 29-31
Articles

Ransomware Attack on Medstar: Ethical Position statement

Najam Ul Hassan University of Maryland University College

Medstar Health was the target of ransomware attack in 2016. The attack impacted the provision of healthcare services to the patient. Medstar opted not to pay the ransom and, instead, responded by shutting down its electronic medical record (EMR) systems and restoring the data from the backups. The paper analyzes the event, Medstar's response and its negligent behavior that allowed the vulnerability to be exploited. The author provides an ethical position statement and recommendation to reduce the chances of any future attacks.

Keywords: Ransomware, Medstar, Crisis management

Introduction

Medstar Health, the largest healthcare provider in Maryland and the Washington D.C. region, was the target of a malware attack in 2016 (*Medstar Health*, n. d.). The attack shutdown the information systems and locked up patient records rendering Medstar Health employees unable to deliver healthcare services to a number of the patients (McCarthy, 2016). The staff had to rely on paper records for patient treatment which 'created chaotic environment in at least one Medstar location' and created a 'patient safety issue' (Cox, 2016). The author, who was a mid-level IT consultant at the time, the event and consequences, response to the crisis and the author ethical position statement about the incident.

Background

In March 2016, hackers used Samas or 'samsam,' a virus-like software tool, to discover that the Medstar uses JBoss application server (LaPointe, 2016). Red Hat's JBoss technology enables programmers to rapidly develop and implement custom software tools throughout the organization (LaPointe, 2016), However, LaPointe (2016) points out that JBoss had a known security issue, which enabled the unauthorized external user to gain control of the computer system.

The hackers exploited the flaw and employed a ransomware to infiltrate and encrypt the data (Reed, 2016). A ransomware is an 'extortive malware that locks user's data in order to get payment for unlocking the data' (Sabillon, Cano, Cavalier, & Serra, 2016). In other words, 'ransomware is malware that locks your computer or prevents you from accessing your data using private key encryption until you pay a ransom' (Richardson & North, 2017). The hackers demanded 45 bitcoins, about $19,000, to provide a key that would unlock the data on all the systems or 3 bitcoins, about $1,250, to unlock on computer (Cox, 2016; McCarthy, 2016). The payment had to be made within 10 days or the key would be deleted, making it impossible to recover the files (Cox, 2016; McCarthy, 2016).

Response to the Crisis

Once Medstar noticed the breach, efforts were made to fix the issue (Reed, 2016). However, when the problem kept on worsening, a midlevel director at Medstar made the 'brave but per-the-protocol' call to shut off all the electronic medical record (EMR) systems (Abdollah 2016; Reed, 2016). Although the decision caused hardship in the provision of healthcare to the patients, it enabled Medstar to stop the malware from spreading. Even though the amount that the hackers demanded was not excessive, Medstar decided not to entertain their demands (Abdollah 2016; Reed, 2016). Instead, Medstar resorted to restoring the data from the backups and were able to reach 90 percent functionality in less than a week (McCarthy, 2016).

Security Issue

Hackers exploited the vulnerable JBoss server application to penetrate Medstar network (Abdollah, 2016; LaPointe, 2016). Security researchers, Abdollah (2016) states, found that JBoss was often configured incorrectly, yielding control to the external unauthorized users. Warnings were circulated, stating that the security issue can 'allow unauthorized users to access confidential information and potentially disrupt business operation' by the US government, Redhat Inc. and others in February 2007 and March 2010 (Abdollah, 2016; LaPointe, 2016). LaPointe (2016) argues that Medstar could have fixed the issue by installing the security patch or by 'manually deleting two lines of software code.'

Ethical Position Statement

The author found that Medstar's decisions to shut down the EMR systems and to not comply with the hackers' demand for ransom were quite commendable. Meticulous system of keeping data backups and pertinent crisis protocols helped the organization to recover relatively quickly. However, Medstar was found lacking in patching the known security holes. JBoss security patch was not applied even though warning was issued almost seven years ago. Medstar needs to improve its patch management procedures. The ransomware crisis exposed the vulnerabilities that existed due to the deficient patching management of JBoss, which was negligent at best.

In order to continue to abide by its values of service, patient first, integrity, respect, innovation and teamwork, Medstar should adopt a three-pronged approach to reduce the chances of any future attacks (*Medstar Health*, n. d.). Primarily, patch management procedures should be updated to ensure that they take into account any warnings issued by the vendors, the government or other security companies. Moreover, Medstar needs to improve its response to crisis situations by improving the disaster recovery plans (DRP) and business continuity plans (BCP). Frequent drills to test these plans should also be conducted to keep the plans up-to-date and to train the staff. As Iovan and Iovan (2016) put it succinctly, 'a skillful fighter is one who not only wins, but excels in winning with ease.' Finally, counter offensive corporate strategies, such as penetration testing, should be implemented to catch the vulnerabilities that can be exploited to cause monetary and other damages (Neal & Ilsever, 2016).

Conclusion

While Medstar was able to come out of the ransomware attack relatively unscathed, a closer analysis of the event, its causes and Medstar's response, point to the areas of improvement. Although the crisis was mostly well-managed, it was the patch management procedures, DRP/BCP and the passive approach to security that needs to be reviewed. It the lessons learned are applied properly, the experience may help Medstar avoid future attacks.

References

Abdollah, T. (2016, April 5). Hackers broke into hospitals despite software flaw warnings. *The Associated Press*. Retrieved from https://apnews.com/86401c5c2f7e43b79d7decb04a0022b4/hackers-broke-hospitals-despite-software-flaw-warnings

Cox, J. W. (2016, March 29). MedStar Health Turns Away Patients After Likely Ransomware Cyberattack. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html?noredirect=on&utm_term=.b8eec6f84dc1

Iovan, S., & Iovan, A. (2016). From Cyber Threats To Cyber-Crime. *Journal of Information Systems & Operations Management*, 425-434. Retrieved from https://search.proquest.com/docview/1861345731?accountid=44888

LaPointe, J. (2016, April 7). MedStar Ransomware Attack Caused by Known Security Flaw. *Health IT Security*. Retrieved from https://healthitsecurity.com/news/medstar-ransomware-attack-caused-by-known-security-flaw

McCarthy, J. (2016, April 4). MedStar Attack Found to be Ransomware, Hackers Demand Bitcoin. *Health IT News*. Retrieved from http://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware-hackers-demand-bitcoin

MedStar Health. (n.d.). Retrieved from https://www.medstarhealth.org/

Neal, P., & Ilsever, J. (2016). Protecting Information: Active Cyber Defence For The Business Entity: A Prerequisite Corporate Policy. *Academy of Strategic Management Journal*, 15(2), 15-35. Retrieved from https://search.proquest.com/docview/1826881224?accountid=44888

Reed, T. (2016, July 6). MedStar Official on Cyberattack: 'We Chose by Design not to Pay the Ransomware'. *Washington Business Journal*. Retrieved from https://www.bizjournals.com/washington/news/2016/07/06/medstar-official-on-ransomware-attack-we-chose-by.html

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), 10-21,101. Retrieved from https://search.proquest.com/docview/1881414570?accountid=44888

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, 4(6), 165-176. Retrieved from https://search.proquest.com/docview/1874038161?accountid=44888