Bryce Forseth

12/2/2024

MIS 374

Written Final Project

**Mitigating Ransomware Threats In Healthcare Organizations**

Ransomware attacks are a growing threat that has significant effects on healthcare organizations. These attacks jeopardize patient care, data privacy, and the operations of the business. Healthcare providers who manage the patient data have been increasingly targeted due to the value of the data. In this project, it will explore ransomware threats to healthcare organizations, and the financial and operational impacts of these attacks.

Ransomware attacks involve malicious software that encrypts the organizations data, locking the users out until a ransom is paid. In healthcare, attackers targeted electronic healthcare records, diagnostic tools, and scheduling tools. The most common attack methods attackers used, “were exploited vulnerabilities (34%) and compromised credentials (34%), up from 29% and 32% of attacks in 2023. Malicious emails (19%) and phishing (9%) were both down from 22% and 14% of attacks in 2023” (Alder, 2024). This information, which was collected in the first three quarters of 2024, describes how attackers have significantly increased their attention to employees credentials, and weak points in the security setup to gain access to healthcare organizations database. After these attacks occur, cybercriminals can deny the, “ability to access electronic health records (EHRs), schedule appointments, conduct diagnostic tests, and share vital information among care teams” (SafetyDetectives, 2024). This can lead to appointment cancellations, treatment delays, and overall delays to the organizations operations. These attacks can present significant risks to patients lives.

Healthcare organizations should be very concerned about the effects of ransomware attacks on their company. In 2019, the USA had the highest average costs for a data breach. “The average cost of a healthcare data breach (average breach size 25,575 records) in the USA is $15 million” (NLM, 2020). That would average to about $587 per record. Cyber security teams for healthcare organizations should be continuously testing and upgrading their cybersecurity, to prevent these costly data breaches. Along with the financial effects, a healthcare organization can also face reputational damage for the leaks of sensitive data, such as social security numbers, patient medical records, and financial details.

To counter cybercrimes, specifically ransomware attacks, healthcare organizations should specifically train and test employees on cybersecurity training. Within cyber security attacks, humans are a main vulnerability in security systems. If healthcare organization’s emphasize training activities, it would start with company training plans. These plans would start by emphasizing phishing emails, practicing safe coherence. The training would teach about sketchy emails, and mitigation practice about specific situations. This would help prevent phishing email attacks, and potentially limit compromised credentials.

**Part Two**

My example for interactive training for the healthcare organization would start with email training. This training would start with internally created games, where employees team up to identify potential scams and earn points. The winner of the training activated would receive a reward, tailored to the healthcare organizations ideas. The game would have multiple different rounds, creating a competitive edge for employees to compete against each other, and understand the effects of cyber security attacks, the risks and costs associated with attacks, to help employees learn and understand the importance of cyber security.

The game would insist on working as a team to identify scam emails, and identify fake messages which would spotlight employees vulnerabilities, where employees become subject to attacks. The game would provide examples of emails, both fake and real, and examine the employees ability to decipher real emails from phishing attempts. This activity would help with phishing attack defense, and also help prevent compromised credentials. When stopping phishing attacks, cybercriminals can’t access employees accounts through malicious links, which helps prevent employees from giving up credentials to unauthorized users.

Sources

Alder, Steve. HIPAA Journal. (2024). *Healthcare ransomware attacks continue to increase in number and severity*. <https://www.hipaajournal.com/healthcare-ransomware-attacks-2024/>

SafetyDetectives. (2024). *Healthcare under siege: Ransomware in 2024*. <https://www.safetydetectives.com/news/healthcare-ransomware-2024/>

Ssh, Adil, Zaour, Mohammod, Alenezi, Mamdouh. (2020). *Healthcare Data Breaches: Insight and Implications*. National Library of Medicine. <https://pmc.ncbi.nlm.nih.gov/articles/PMC7349636/>