JUSTICE INSTITUTE of BRITISH COLUMBIA

RELEVANT
FOCUSED
READY

Post-Secondary Institutions Being Cyber-Aware

Darlene Sunderland

Introduction

Cyber-criminal attacks on higher education facilities are becoming common; these attacks have the potential to negatively impact thousands of innocent people. The topic for this research was chosen to determine the most likely attacks, and mitigation strategies security departments in post-secondary institutions should consider when protecting data and networks from malicious intent. The research question was therefore determined to be: “What are the most likely cyber-attacks in relation to a security department at a post-secondary institution, and how can these risks be mitigated?”

Background

Cyber-attacks in businesses, personal and educational arenas are becoming more common each day. There are daily news articles outlining the latest post-secondary attack(s) and the resulting damage caused. There seem to be many types of attacks and the results can be varied depending on what cyber-criminals were after. In some cases there can be privacy breaches, in others, operations can be disrupted, or assets can be frozen until ransoms are paid. If cyber-criminals obtain access to secured data via a network breach there could be loss of information and or financial loss, and legal issues resulting from loss of data or money. Cyber-attacks are a problem that is likely to increase as our world becomes more dependent on technology.

Methods

The literature researched for the project consisted of secondary data. The search was conducted for online sources that could provide insight on both historical and current cyber-attack trends, and mitigation strategies security departments at post-secondary institutions should consider for protecting data and networks. Articles, newsprint, conference(s) reports, post-secondary theses, government documents and scholarly research documents were considered and reviewed. A critical appraisal of the information was performed in reaching the final results.

Results/Findings

After reviewing the data, it was determined that security departments at post-secondary institutions are most likely to see ransomware, distributed denial of service (DDoS) and phishing as cyber attacks (Biddle, 2017; Singh & Joshi, 2016). Each of these has the potential to slow down or stop campus services and activities or result in a breach of student data. These cyber-attacks could affect services such as phone access, egress, and emergency systems managed electronically. Ransomware malware encrypts user files, rendering them useless until a ransom has been paid (Simon, 2016). DDoS involves the use of multiple networks and computers to carry out an attack that overwhelms the targeted network, and phishing is a targeted attack where the criminal sends an email with a link that can either introduce malware, or encourage the user to enter personal information (Biddle, 2017).

Discussion

After reviewing the literature, types of attacks and impacts to a security department, it was determined that ransomware, DDos and phishing are the most likely attacks (Biddle; Polyakov, 2017). These attacks could affect a security department in a number of ways. Ransomware could result in online systems no longer working – this could affect entry points into buildings, bring down security cameras and make it impossible to look up information for students who need help or who could be causing trouble (Neuman, 2009). DDoS could affect the security emergency system on campuses resulting in emergency services delay such as: information processing of potential errors with the access software and emergency networks linking fire, police and ambulance to the campus emergency alert system. Phishing attacks could lead to the loss of private information, which is held in large amounts by post-secondary institutions (Diaz Anderson, Wolak & Opderbeck, 2017). This could include private campus body information, or various types of systems information. There is also the risk of malware infection from links included in phishing emails (Polyakov, 2017). Each of these potential risks must be considered and mitigated by the security department and post-secondary information technology (IT) personnel.

Conclusions or Recommendations

In order to respond to the risks noted in the discussion above, Simon (2016) recommends introducing email security protocols in place and training staff to be suspicious of links and report these emails immediately. Further suggestions include monitoring key stakeholders’ devices for criminal activity, and avoiding peer-to-peer file sharing over networks (Simon, 2016). Diaz et al. (2017) discuss the importance of having plans in place to mitigate open storage sites from cyber-attacks (Diaz et al., 2017).

Singh and Joshi (2016) recommend understanding the weaknesses and upgrading networks on a regular basis, and being proactive instead of reactive. They also recommend that IT should track users’ log-ins to high-risk websites on university networks (Singh & Joshi, 2016). Constant awareness and learning is essential for all security department and IT staff as risks from cyber attack are likely to continue to increase due to the high reliance post-secondary institutions place on technology.

References

Biddle, S. (2017, October 6). Common types of cyberattacks in education and what we can learn from them. [FortinetBlog]. Retrieved from https://blog.fortinet.com/2017/10/06/common-types-of-cyberattacks-in-education-and-what-we-can-learn-from-them

Diaz, L. J., Anderson, M. C., Wolak, J. T. & Opderbeck, D. (2017). The risks and liability of governing board members to address cyber security risks in higher education. Journal of college and university law. 43(1) 49-75. Rutgers Law School. Retrieved from http://jcul.law.rutgers.edu/2017/01/the-risks-and-liability-of-governing-board-members-to-address-cyber-security-risks-in-higher-education/

Neuman, C. (2009). Challenges in security for cyber-physical systems. Center for computer systems security information sciences institute university of California. Retrieved from http://cimic.rutgers.edu/positionPapers/CPS-Neuman.pdf

Polyakov, A. (2017, August 21). What cyberthreats do higher education institutions face? *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/08/21/what-cyberthreats-do-higher-education-institutions-face/#67f8d96d640d

Simon, N. (2016). The rising face of cyber crime: Ransomware. Bitsight. Retrieved from https://info.bitsighttech.com/bitsight-insights-ransomware?hsCtaTracking=7dce0bd9-bf5d-456c-ab5e-134a1e47cb7d%7Cd54507aa-4e0d-42d3-9d81-b726f0a0f783

Singh, U. K. & Joshi, C. (2016). Information security risk management framework for university computing environment. *International Journal of Network Security*. 19(5), 742-751. Retrieved from http://ijns.femto.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p742-751.pdf

Bachelor of Emergency and Security Management   Justice Institute of British Columbia   April 2018