Individual Essay

Humans' attitudes, cultures, behaviors, beliefs, and decisions represent a mystery to the cybersecurity team. Humans are the weakest link in information systems security (Cano, 2019). Although organizations put endless technical efforts and complex security policies to protect their clients' data, people have a high probability of exposing the organization's system weaknesses (Dreyer et al., 2018). To protect sensitive information, creating awareness and training are essential (Cano, 2019). Even though cybersecurity education is provided and systems designed to keep information secure and measures put in place to control the behaviors, vulnerabilities intensified by people happens.

System vulnerabilities may result from omission, errors, or deliberate attempts to compromise sensitive data in an organization (Bada, Sasse, and Jason, 2019). Most individuals have grave concerns for the security of their data when using web applications (Zang and Deng, 2017) To ensure that Queens Medical clinic ASMIS is usable, functional and secure, the information technology systems team should address the major human factors including lack of appropriate access control and awareness, and carelessness. Usability, functionality and security should be kept in balance and in a way that they allow the system to achieve its objectives (Reynaga, Chiasson, and van Oorschot, 2015)

Inappropriate access control aims to prevent unauthorized use of credentials to acquire confidential patients' data. It can arise from human factors associated with phishing and spear phishing, scan and exploit pose the highest cybersecurity risks. Such human factors include an automated click response, spoof login page, and socially engineered access to login credentials. Phishing human factors trick a human target, mostly an employee, into clicking on an infected attachment or opening a link to start the chain of compromising the system (Agazzi, 2020).

These factors usually target users with access to information systems and acquiring their login credentials.

Human factors associated with scanning and exploitation involve hackers attempting to gain as much information as possible about their target and taking advantage of the discovered vulnerabilities to carry out the attack. The information collection phase is considered the recon phase, which can include a port scan which aims to identify open ports in an information system, a vulnerability scan, which follows the port scan and aims to identify vulnerabilities associated with the port identified to be open, and finally the exploitation phase where the attacker uses the identified vulnerabilities to gain access to the system (Boer, 2002)

Moreover, human behaviors, such as making irrational or opinion-based decisions (Johnson, 2021), lack of security awareness of the current cybercrime techniques and carelessness make employees more susceptible to these attacks (Karlof, 2009). Carelessness of the system administrator or any other staff member with access to the system and lack of security awareness can lead to both accidental or malicious exposure of patients' data. These can be mitigated by restriction of important data access to a few staff members, limitation of read and write privileges of data and constant monitoring of the external footprints that might indicate data exposures (Treu and Ira Winkle, 2017).

In addition, automated click response human factor is a phishing attempt mainly present in emails sent to employees such as Queens Medical Centre information technology department or any other employee with access to its appointment and scheduling management information system. It can be in the form of a malicious link or an attached file that collects as much data concerning the targeted individual as possible and sends it back to the attacker. To overcome

this, the hospital's employees should be constantly trained to identify such malicious emails and take the necessary action to address them.

Training should provide information (Cano, 2019) on the hospital's processes and data protection mechanisms. It ensures that employees with access to the information system understand how they are required to handle the data collected (Cano, 2019) from patients to ensure its safety and potentially avoid data loss or unauthorized access. Additionally, measures should be put in place to ensure instructions on data handling are followed and consequences of going against the set procedures be put in place. Different training should be carried out depending on the level of access of employees and regular reminders to be on the lookout for phishing attempts in their daily practices (Cano, 2019).

Furthermore, Queens Medical Centre receptionists and doctors interacting with the information system might have risky beliefs, practice risky behaviors, not feel adequately motivated or use the available technology inefficiently (Badie and Lashkari, 2012). With the help of the management, the information technology team should train them and raise awareness on the best practices while using the system and how to ensure the safety of patients' data. The team should also ensure that patients understand how their data is treated, what measures are put in place to ensure the data is secure. Additionally, patients should be allowed to have access to multiple factor authentication while logging in to their hospital accounts. This will play a significant role in preventing unauthorized access to patients' accounts.

Reference list

Agazzi, A.E. (2020). Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them. *arXiv:2006.00577 [cs]*. [online] Available at: https://arxiv.org/abs/2006.00577 [Accessed 28 Oct. 2021].

Bada, M., Sasse, A.M. and Jason (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *arXiv.org*. [online] doi:10.48550/arXiv.1901.02672.

Badie, N. and Lashkari, A.H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. *undefined*.

Boer, R. (2002). A Generic Architecture for Fusion-Based Intrusion Detection Systems. *undefined*. [online] Available at: https://www.semanticscholar.org/paper/A-Generic-Architecture-for-Fusion-Based-Intrusion-Boer/c2f9ce7c02a6b4fac7ce3030c49398d18b5853ec [Accessed 4 Jul. 2022].

Cano, J.J. (2019). *The Human Factor in Information Security*. [online] ISACA. Available at: https://www.isaca.org/en/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security#:~:text=The%20literature%20available%20to%20date%20on%20the%20human,of%20individuals%20in%20an%20effort%20to%20protect%20information. [Accessed 4 Jul. 2022].

Johnson, J. (2021) *Designing with the Mind in Mind Simple Guide to Understanding User Interface Design Guidelines*. 3rd ed. Waltham, MA: Morgan Kaufmann.

Reynaga, G., Chiasson, S. & van Oorschot, P.C. (2015) Exploring the usability of captchas on smartphones: Comparisons and recommendations. *In NDSS Workshop on Usable Security USEC.*

Sasse, A.M, & Rashid, A. (2019) *Human Factors Knowledge Area*. Issue 1.0. CyBOK.

Treu, A. and Ira Winkle, G. (2017). Malicious Insider - an overview | ScienceDirect Topics. *www.sciencedirect.com*. [online] Available at: https://www.sciencedirect.com/topics/computer-science/malicious-insider [Accessed 21 Feb. 2021].

Zhang, X.J., Li, Z. and Deng, H. (2017) *Information security behaviours of smartphone users in China: an empirical analys*is. The Electronic Library.