Tabish Parkar

Summative Assessment 2: Ethical Hacking

05HA2309970

Bellville

As Innovatech Solutions begins its journey to have bigger operations into the cloud, it will face various cybersecurity constraints and issues related to this transition. Cloud migration allows for great benefits, namely enhanced scalability, agility along with cost-efficiency. These advantages however do come with security risks for example data breaches along with unauthorized access. This research essay will transverse and explore the key concepts of cybersecurity in cloud systems, scanning key areas for example cloud migration, encryption, vulnerability assessment, identity and access management, social engineering along with cloud-specific threats. It also brings effective strategies to improve their cybersecurity position along their transition to the cloud.

Cloud migration includes moving data, applications and workloads to cloud-based environments. While this provides many advantages, it could also raise major security concerns. The most common issues include data breaches and unauthorized access, often stemming from usual security measures that highlight mainly on on-site data centres. Organisations such as Innovatech will need to adopt a total understanding of their data assets and the possible constraints in cloud environments. A good strategy allows for emphasising the selection of verified cloud deployment models which are public or private and hybrid which places itself along with the companies mentioned security needs and complicity needs.

Encryption acts as a critical element in protecting highly important data, mainly during cloud migration. It safeguards data from unauthorized access by transforming information into an unreadable format unless decrypted with the proper keys. It is critical that Innovatech Solutions upgrades their encryption methods. Which should include simultaneously fostering symmetric and asymmetric cryptography to have surety in robust data protection. Symmetric encryption allows for the same key to be used for decryption and encryption, while asymmetric encryption makes use of a pair of keys (public and private keys) which offers a more protective approach mainly for complex environments needing more advanced key management strategies.

Conducting vulnerability assessments is important to find any weaknesses in a cloud environment before probable attacks occur. Assessments should feed focus on the understanding of the specific cloud infrastructure used, analysing configurations, access controls along with already existing security measures. Regular vulnerability assessments also help Innovatech Solutions discover and manage risks predictively, which ensures that their cloud infrastructure remains safeguarded against rising threats.

Effective identity and access management are vital in cloud security. It entails surety when the right individuals have the appropriate access to cloud resources. A lack of strong identity and access management practices could proceed to unauthorized access, data leaks along with other security constraints. Fostering multi-factor authentication will highly strengthen security against any unauthorized access by allowing for users to present two or more verification factors. Innovatech should also consider adopting role-based access controls to manage permissions based on roles within the organization which reduces the risk of internal threats.

Human error remains as one of the weakest points in cybersecurity. Social engineering methods such as phishing attacks, exploits their vulnerability by misleading employees into dispensing sensitive information. Providing compulsory and constant training for employees on identifying and managing social engineering threats is vital. The training should cover the best methods, how to respond to dubious activities and strengthening of a security-aware culture within the company.

Cloud systems oppose unique threats, counting data breaches, denial-of-service attacks and insecure APIs'. Data breaches can cause significant losses, both reputationally and financially. Innovatech Solutions needs to adopt a durable incident response plan which gives clear steps to identify, respond to and recover from security breaches. Furthermore, the adoption of robust security tools such as cloud access security brokers and continuous monitoring solutions can also aid in shielding against rising threats and weaknesses.

Expanding into a cloud environment presents both substantial opportunities and significant cybersecurity challenges for Innovatech Solutions. By addressing key areas such as cloud migration risks, enhancing encryption practices, conducting regular vulnerability assessments, implementing effective identity and access management, and training employees on social engineering defenses, Innovatech can bolster its cybersecurity posture. Moreover, establishing a strong incident response plan and utilizing advanced security tools will help mitigate the risks inherent in cloud computing. As Innovatech transitions into this new digital landscape, prioritizing cybersecurity will be essential to protect its valuable digital assets and maintain compliance with industry standards.

Reference List

Gadde, H. 2021. Secure Data Migration in Multi-Cloud Systems Using AI and Blockchain. International Journal of Advanced Engineering Technologies and Innovations, 1(2):128-156. Retrieved from: https://d1wqtxts1xzle7.cloudfront.net/119017263/128_156_ijaeti_2021libre.pdf?1729402754=&response-contentdisposition=inline%3B+filename%3DSecure_Data_Migration_in_Multi_Cloud_Sys.pdf&Expires=1738219588&Signature=VEVCBbd7wmzTCQ6VglGq7np09SbPUvKAchajsdkaOEPf697dbaIERRePLYilS~~h2lxl9KgLU6nx~Ov4BLOjm0dFDxMjfJRDUqTPVeqhZ6XTCGQFQ9...[Accessed 25 November 2024].

Kushwah, V.S. & Saxena, A. 2013. A security approach for data migration in cloud computing. International Journal of Scientific and Research Publications, 3(5):1-8. Retrieved from: https://www.researchgate.net/profile/VirendraKushwah/publication/236658752_A_Security_approach_for_Data_Migration_in_Cloud_Computing/links/00b7d518bd18762b30000000/A-Security-approach-for-Data-Migration-in-CloudComputing.pdf [Accessed 3 September 2024].

Alsirhani, A., Ezz, M. & Mostafa, A.M. 2022. Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing. Computer Systems Science & Engineering, 43(3). Retrieved from: https://cdn.techscience.cn/ueditor/files/csse/TSP_CSSE43-3/TSP_CSSE_24854/TSP_CSSE_24854.pdf [Accessed 3 September 2024].