Tabish Parkar

Summative Assessment 2: Systems Development 2B

Bellville

The arrival of cloud computing has changed the landscape of data storage and accessibility, which allows companies to grip sizeable resources along with reducing operational expenditure. But this change partners itself with special needs for network security. As companies move to cloud systems, they discover new weaknesses that can reveal important information. We will discuss the two main challenges that companies or organisations face.

Challenge 1 - Data Breaches Along with Unauthorized Access

One of the most urgent issues alongside cloud migration is the higher probable risk of data breaches and unwanted access. When companies put sensitive information in cloud systems, they voluntarily expose themselves to threats from cybercriminals who may exploit weaknesses in the cloud environment. Data breaches can happen due to vulnerable access controls, weak encryption from developers and an error in security settings. Furthermore, the shared responsibility model in cloud computing may confuse security; while cloud service providers are obligated to keep security of the cloud infrastructure, companies need to also control the security of their data in that infrastructure.

To defend against the risk of data breaches and unwanted access, companies should foster advanced access management or controls along with strong encryption methods especially to the firewall. An important part that extends security is multi factor authorisation which needs users to show various methods of certification before gaining access to data. With the application of strict identity and access management policies, companies can manage access to important data to specific employees which need it for their tasks.

Furthermore, encryption is important when it comes to data protection whether it be at rest or in transit. Companies are suggested to foster an algorithm with strong encryption to make sure that even if data is attacked while being sent or opened without authorization, it stays indecipherable. Implementing an end-to-end encryption can also greatly lower the chance of data breaches, this ensures that only verified users can decrypt and open important information.

Challenge 2 - Compliance and Regulatory Issues

Another recognised issue in cloud migration is going through compliance and regulation requirements. Companies in different fields are obligated to follow the strict rules and regulations when it comes to data protection and privacy. When migrating to cloud infrastructure, organizations must verify that their cloud service providers comply to these rules and regulations that data handling practices align with legal obligations. Not meeting up with these standards could result in serious penalties and damages to a company's reputation.

To tackle compliance challenges, companies need to implement regular compliance checks and precise assessments of their cloud service providers. This means that the company must constantly verify the cloud service providers security qualifications, data handling methods and their compliance to industry rules and standards. Companies could suggestively also agree on clear contractual agreements with cloud service providers that profile ownership of data, security responsibilities along with obligations to meet industry compliance and standards. Furthermore, companies could also have a grip on compliance management tools which help to automate the tracking and reporting of the compliance standards. These tools could also help to identify potential compliance issues and help to verify that data protection methods are always being implied over every cloud service.

In closing, while cloud computing gives an impactful advantage with regards to data access and operational productivity, it can also introduce highly important challenges that come with networking security. Unwanted access via data breaches and compliance issues are two of the main weaknesses that organizations are plagued by and must face as they move to the cloud. By applying advanced access controls or management, strong and robust encryption, constant compliance checks and proper assessments of cloud service providers, companies can also manage these issues to ensure secure data access control in cloud infrastructure. With time passing and the virtual sphere continues to develop, implementing security methods will be a necessity for companies looking to grip the full power of the cloud industry whilst protecting their important and highly sensitive data or information.

References

Anas, B., Asmae, B., Nour el houdo, M. and Mohammed, G. (2012) 'Cloud computing: Security challenges'. Available at: https://www.researchgate.net/publication/261447405_Cloud_computing_Security_challenges (Accessed: 19 March 2024).

Ertaul, L., Singhal, S. and Saldamli, G. (2013) 'Security Challenges in Cloud Computing'. Available at: https://www.researchgate.net/publication/267697749_Security_Challenges_in_Cloud_Computing (Accessed: 19 March 2024).