University of Essex Online

Launching into Cyber Security January 2021

Collaborative Learning Discussion 1

Summary Post

The last two weeks' discussion was on how e-commerce becomes a big part of people's lives and how important it is to get high secure transactions to protect customer data and business financial transactions. The transaction traffics contain bank, debit or credit card details and some customers data. Similarly, the companies have a big challenge to encrypt the transaction packet at a high encryption level and ensure it is safe.

(Kou,2013) The latest technological advances in complex online services have required stronger security and more convenience in online payment over the internet.

The point mentioned by Vaibhav is partially correct; the transaction usually split into two parts. (Chawla, 2021). The fully cloud-based deployments are still not recommended by big e-payment companies, because most companies do not trust to keep the critical data under Cloud Service Providers risk. Based on that, several of them still hosting the databases and critical systems in their own data centres.

Back to Joseph's post, the e-commerce organisations lost billion every year by the frauds on online payments and forced the organisations to protect the infrastructure and make sure no vulnerabilities that can be the easy way or any cybercrime to use it to breach the data(Olaseni, 2021).

Security standards are the recommended way for e-commerce organisations to protect the infrastructure. All IT teams should work very closely with the Cybersecurity team, do regular penetration tests for internal and external connectivity, and keep upgrading the encryption and hashing payments packets.

Furthermore, Anum mentioned that e-commerce websites should be more secure. Most company websites with electronic payments features have a greater possibility to lose the customers and break the trust to use the website again. (Rashid, 2021).

(Anagnostopoulos,2021) describes that the use of encryption and Biometrics can add more security to electronic payments, but not all people can agree to give personal data like that. Also, it is risky if the company has any breach and all Biometric data stolen.

References:

- Kou, W. (2013) Payment Technologies for E-Commerce. Germany: Springer Berlin Heidelberg. Available from: https://www.google.co.uk/books/edition/Payment_Technologies_for_E_Commerce/wwJJCAAAQBAJ?hl=en&gbpv=0 [Accessed 12 February 2021]
- Chawla, V. (2021) Initial Post by Ahmad Alkam, 02 February Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240022

- Olaseni, J. (2021) Initial Post by Ahmad Alkam, 02 February Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240022
- Rashid A. (2021) Initial Post by Ahmad Alkam, 03 February Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240022
- Anagnostopoulos S. (2021) Initial Post by Ahmad Alkam, 11 February Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=240022