Security Requirements Specification

Ecommerce has become a staple within the everyday life of a human being. Day in and day out we participate within ecommerce without much thought behind it. In this case a Shopify API is the focus of this topic, to briefly summarise how this API functions. “The ShopifyAPI library allows Python developers to programmatically access the admin section of stores. Data is sent in the XML format over HTTP to communicate with Shopify” (Shopify, 2012). Below will be security requirements for this API to have it function with minimal risk.

User Access

The first barrier to security is who is able to access the system. Users should be defined with their own unique usernames along with passwords. As well as this two-step verification is required and can be easily implemented with an app such as Microsoft Authenticator which “helps you sign in to your accounts when you're using two-step verification. Two-step verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised” (Microsoft, no date).

Data Encryption

Since an ecommerce platform will hold customer data and data about products a big requirement will be to have the data encrypted, this will protect sensitive data such as payment information, personal information and logistical information too. Not having data encrypted could pose a big threat to the function of the API and the systems connected to the API.

Monitoring and Recording Activity

The usage of the API assigned should be monitored and logged on a regular basis. Doing this would allow anomalies to be detected and will allow suspicious activity to be detected.

Compliance

With GDPR being EU law which is also applicable in the UK, these laws must be adhered to. “The GDPR contains many principles for processing, collecting, accessing, rectifying, erasing, and transferring personal data. But it is its specific regulations on securing and protecting data that concern those responsible for organizational information and data security” (Loureiro, 2023). It is essential that the implemented API adheres to GDPR, not doing so can result in fines and sanctions.

Conclusion

The above security measures are designed to be applicable to the unique security challenges that an ecommerce platform can encounter. It is vital and important that factors such as compliance, data protection and authentication are focused on and prioritised, this allows trust, safety and the prevention of any risks becoming major incidents. It’s best to prevent a problem from occurring rather than solving an issue once it has occurred.

Reference List:

Loureiro, N.L. (2023) *What is GDPR compliance in web application and API security? - probely*, *What is GDPR Compliance in Web Application and API Security?* -. Available

at: https://probely.com/blog/what-is-gdpr-compliance-in-web-application-and-api-security (Accessed: 17 February 2024).

Microsoft (no date) *Microsoft*, *Microsoft Support*. Available at: https://support.microsoft.com/en-gb/account-billing/download-and-install-the-microsoft-authenticator-app-351498fc-850a-45da-b7b6-27e523b8702a#:~:text=The%20Microsoft%20Authenticator%20app%20helps,forgotten%2C%20stolen%2C%20or%20compromised. (Accessed: 17 February 2024).

Shopify (2012) *Shopify_python_api*, *Shopify Open Source > shopify_python_api*. Available at: https://shopify.github.io/shopify_python_api/ (Accessed: 17 February 2024).