Cybersecurity Report

Jake Meaker

This report will discuss the key cybersecurity issues for the company “XYZ Games” and some control strategies for the mitigation of these concerns. It will also outline the major GDPR that currently exist within the company. After reviewing the cybersecurity report for “XYZ Games”, many cybersecurity issues have been found. Many of these are very severe and ways to solve them will be discussed later.

The issues and why they are concerning are:

* The Customer Service team share a single account for accessing customer details to deal with issues. This includes login issues, credit card and payment issues, purchase failures, and refunds. This is a severe cybersecurity concern for the company. If the access details for this database are hacked or gained via other means, then all the player payment details will become vulnerable to exploitation.
* Several USB data sticks have been lost by a member of the company. This is also a severe cybersecurity risk for the company. Whilst it is believed that no one will know what to do with their customer data, the data hasn’t undergone any encryption and can likely be deciphered easily. Data is also a very valuable resource and customer data can be sold or used for blackmail/manipulation.
* Putting data on USB sticks for data transferal is also a cyber concern. The data can be transferred via digital means, provided appropriate security is on those systems.
* Having one database to store the data, that is accessible to everyone within the company, and no security for it have been mentioned. This means that all this data is accessible by anyone and could be hacked or stolen by and employee and no one would know who did it.
* Development on a single main branch. This can cause issues as it leaves all the game features exposed if there was a cyber-attack from one of the company’s competitors, allowing them to spy on or steal from the company, resulting in lost Intellectual Property
* Development backups are managed on git. A problem with this is that if the version-controlled backups were accidentally, or intentionally, deleted, then the ability to retrieve them is gone and potentially even access to previous versions.
* Second-hand equipment that is still running the same software as when it was acquired can cause many issues. The equipment may contain data previously stored on them. They also may have software left on them from the previous owner that could allow that owner access to the equipment.
* The second-hand equipment also is running many different Windows OS versions and different application versions. This is bad practice as updates for these usually contain the most recent protection for known viruses and malware. Also having mismatched application versions can cause many issues when trying to collaborate on a project and this can lead to lost time and removes the ability for the developers to work on the game.
* There is no dedicated IT Department and programmers from other areas are fixing problems as they arise. This can lead to irregular fixes and common practices. There is no set standard problem-solving system and fixes may only be temporary. This also removes that employee from their own work, obstructing production.
* The final and possibly most important problem is that the CEO of the company believes that cybersecurity practices would slow the company down. This is, however, untrue, as the problems caused from the lack of cybersecurity would cause the company many severe issues and would halt, or even erase progress.