Cybersecurity Report

Jake Meaker

Section 1

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.

1. Sharing a single account for accessing customer data.

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. For example, on April 20th, 2011 Sony’s PlayStation Network was attacked by hackers losing the company $171 million while the site was down, and costing a further $15 million in settlements after a class action lawsuit over the breach (Armerding, 2018)

2. USB Sticks containing customer data.

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. This can cost the company a large amount of money. An example of this is from October 2017 when a member of the public found a USB which had been lost by an employee of Heathrow Airport Limited. The member of the public was able to view the information on the stick at a public library. Data stored on the USB at XYZ has not been encrypted so this could also happen. It cost Heathrow Airport Limited £120,000 in fines from the Information Commissioners Office (Information Commissioners Office, 2018). Also, using USB sticks as a method of transportation is an outdated and inefficient method of transporting data which is a breach of GDPR which could result in large fines.

3. Single Database for storing Data

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. It could easily be attacked via SQL injection, Configuration errors, and privilege abuse. Breaking into a database is easy. “It takes the average attacker 10 seconds to hack in and out of a database” (Higgins, 2008) Having data hacked can cost the company a lot of money too. An attack on Heartland Payment Systems cost the company over $300m. (Vass, 2018)

489 words

4. External git backups

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. Ineffectual backups and the inability to retrieve data could be catastrophic. GitLab, a company that provides these kinds of services, had this happen to them, which caused them to have to rebuild their systems (Sharwood, 2017). Also having customer data on the git leaves it exposed to anyone who can hack it. Passwords for systems, such as git, rely upon passwords for access which can be broken surprisingly easily. Hackers can test words against passwords at a rate of 8 to 10 billion per second (Computerphile, 2016).

5. Second-hand Equipment

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. Even if the equipment has been wiped, there are still issues as refurbishing doesn’t eliminate Trojans or malware from the equipment (Armerding, 2015). 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. It is also considered a breach of GDPR which could result in a large fine. (Parker Software, 2018)

6. Lack of IT Department

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. GDPR also explicitly requires that staff are trained in GDPR. The fines for not having this in place is 4% of annual global income or 20 million euros, whichever is more (Morelli-Green, 2019).

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.

426 words

GDPR issues based on current operations.

GDPR applies to all companies and organisations that are operating within the EU and that process data about EU residents. XYZ is legally obligated to be following GDPR as they are operating within this area. If the company continues not following GDPR then it could result in a fine of 20 million euros or 4% of the company’s worldwide profit, whichever one is more.

Under GDPR it is also now mandatory that companies notify the authorities if there is a breach of data within 72 hours of first becoming aware of the breach. They must also notify the customers immediately upon finding a breach. XYZ has currently breached this part of GDPR with the loss of USB sticks containing customer data, and therefore could result in the fine. Customers also have the right to obtain confirmation from XYZ information on the processing of their data and what it is and isn’t being used for. Also, the company is, upon request of the customer, to provide the customer with a digital version of the personal data that the company has, free of charge.

The customer also has the right to have their data erased by the company. The company will then cease any action that are being taken with their data must stop and third parties should halt processing of the data. The conditions of this, found in Article 17 (Information Commissioners Office, Right to erasure), state that the customers data is no longer relevant to the original purpose and that they have withdrawn their consent.

Under GDPR, companies should be including “Privacy by Design” from the initial design of their systems to include data protection, rather than adding it later. Specifically they should be implementing appropriate systems and company organisation measures to meet the GDPR requirements, protecting their customers data. Article 23 states that controllers must only hold and process data that is essential for their processes.

Under GDPR companies that are dealing with large amounts of customer data and special data must have an appointed Data Protection Officer. It is their responsibility to must be provided with required resources for their tasks and their knowledge must be maintained. They also must report directly to the highest level of management. They also are not allowed to carry out any tasks that would result in a conflict of interest.

394 word

Bibliography

ARMERDING, Taylor. 2018. ‘The 18 biggest data breaches of the 21st century’ CSO from IDG

Available at: <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html> [accessed 16/11/2019]

INFORMATION COMMISSIONERS OFFICE, 2018. ‘Heathrow Airport Limited fined £120,000 for serious failings in its data protection practices’

Available at: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/heathrow-airport-limited-fined-120-000-for-serious-failings-in-its-data-protection-practices/> [accessed 16/11/2019]

HIGGINS, Kelly Jackson. 2008. ‘Hacker's Choice: Top Six Database Attacks’ Dark Reading

Available at: <https://www.darkreading.com/risk/hackers-choice-top-six-database-attacks/d/d-id/1129481> [accessed 16/11/2019]

VASS, Lisa, 2018. ‘Hackers sentenced for SQL injections that cost $300 million’ Naked Security

Available at: <https://nakedsecurity.sophos.com/2018/02/19/hackers-sentenced-for-sql-injections-that-cost-300-million/> [accessed 16/11/2019]

COMPUTERPHILE (2016, July 13). Password Cracking – Computerphile [Video file]. Retrieved from [<https://www.youtube.com/watch?v=7U-RbOKanYs>]

SHARWOOD, Simon. 2017. ‘GitLab.com melts down after wrong directory deleted, backups fail’ The Register. Available at: <https://www.theregister.co.uk/2017/02/01/gitlab_data_loss/> [accessed 16/11/2019]

ARMERDING, Taylor. 2015. Second-hand devices – cheaper but risky’ CSO from IDG

Available at: <https://www.csoonline.com/article/2908363/second-hand-devices-cheaper-but-risky.html> [accessed 16/11/2019]

MORELLI-GREEN, James. 2019. ‘GDPR explicitly requires staff training, yet many are still at risk’ Engage in Learning. Available at: <https://www.engageinlearning.com/blog/legal/gdpr-requires-staff-training-in-place-yet-many-at-risk/> [accessed 16/11/2019]

INFORMATION COMMISSIONERS OFFICE, ‘Right to erasure’

Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/> [accessed 16/11/2019]

159 words