Business report regarding the cybersecurity of a company XYZ report.

**Introduction**

In this essay I am tasked to assess the current operations of a game company and to point out the relative issues with their modus operandi, to then propose relative solutions to their security faults. Also, I am going to provide a list of major issues they are going to encounter if they will continue to be non-GDPR compliant.

At the end of the company assessment, I will provide some code demonstrations comparing the Caesar and XOR

ciphers against modern AES standard cryptography in order to demonstrate why the modern AES standard is a superior approach to cryptography than its much older competitor.

**Part 1: the security flaws of the XYZ company.**

1. The Company marketing team use the sign-up details of their consumers and data-mines the server in order to sell the players in game items and other micro-transactions tailored from the trends of their activities in the game. The main issue is that the data mining are done without the user consent, which breaches the article 7 of GDPR[1], which forbids the processing of the data without the User's consent. In recital 32 of GDPR, the user must give full consent to any kind of data processing the company might be interested to do, to cite recital 32 "Silence, pre-ticked boxes or inactivity should not therefore constitute consent.".
2. The company passes sensible data (customer names, emails, billing addresses and bank details) through likely not encrypted USB which has been reported that they have be lost several times during the company lifespan. The loss of this data can dramatically damage the studio to the point of bankruptcy, has failing to report can land the studio with a fine by the GDPR administration up to 10 million euros or 2% of your global turnover.[2]

3. The company has only one account for managing the sensible data of the costumers, which, the credentials to access this account are shared between every member of the marketing team. This could rend the company liable for more sensible data leak, has, any person can access this account and steal any data from its recipient, and, because it’s only one account, it would be difficult to impossible track the potential offender.

4. The relative absence of security protocol and training by the company to its staff members. This is one of the major problems the company is facing now, as at the event of any data breaches the company would not know how to react. Has article 32[3], the company must provide a robust, state of the art protection of the data with relative security protocols in order to protect its costumer’s privacy.

5. The use of public accessible repositories to store the backups and the current versions of the game source code. The use of publicly accessed repository can become dangerous on the run of the game, as it’s likely the company might involuntarily share files that are not meant to be shared by the company, or worse sharing the SSH files which would grant full access to the repository database of the company to potentially malicious third parties.[4]

6. The operation team shares the same repository service as the programmer team in order to be able to live patch any problem with the game while it’s running on the server. This could arise multiple issues, as the operation team is tasked to maintain the game live on the server, and not to touch code that they might not had any training with it. The likelihood of creating or worsening the bug is increased and might disrupt the service for both the players and the studio, increasing the time the server might be offline to allow the programming team to repair or revert the changes made by the operation team.

**Part 2: Proposing solutions to their main problems.**

1. The marketing team needs to provide to the costumers, at sign up, the request to handle their sensible data, providing information in what they will use the data (e.g.: the data will be used for marketing researches to improve the player experience etc etc) and request if the player would like to receive any emails by the company regarding Marketing offers. All of this must be done following the principles provided by the GDPR commission.[1]

2. The use of portable devices should be replaced by data interfacing between the servers database, allowing the employee, with their own account provided by the company using a state of the art VPN[5], to read them and modify them from their own station without having to move or transport the files in a multi-media storage, exposing the data to a risk to be leaked or stolen. In the occasion certain data has to be transported through a multimedia file, the files need to be encrypted and the person carrying it has to report straight away if the USB has been lost, so that the company can report the data leak to the GDPR commission facing less if no charges by the surveying body.[6]

3. The company should provide every employee in the customer service department with their own accounts to allow them to interface with the Customer Database. It is set in this way in order to survey and pinpoint accurately which employee has accessed certain information or changed data and allowing the surveying body to find the potential offender.

4. The Company must create security protocols in order to maintain the safety and the secrecy of their costumer’s sensible data and their product source code. They need to hire IT technicians to set state of the Art fire Walls and VPNs, create a Service-level agreement for the use of the company’s server and to provide training to every employee for the clean and safe work with the company’s software and the handling of sensible data.[3]

5. They need to implement a private accessible repository, such as: EWS, COD Commit and Bit Bucket in order to maintain their code safe from the being spied or modified by malicious party, preventing industrial espionage and to prevent incidents such as the UBER incident, where Hackers managed to access Uber’s server cloud by peering in the source code that was at the time stored in a public accessible repository.[7]

6. The operation team should, instead of live patching any bugs, is to report them to the programmer teams, then decide if it’s worth waiting for a new patch Update or to momentarily offline the server if the bug in question is game-breaking or could be a possible cyber-security hazard. Both teams should not be allowed to interface each other systems, in order to prevent cross over or corruption of data between the parties.

**3: The possible GDPR Issues**

The main GDPR issues this company faces are how they handle their customers sensible data, the commonly reported loss of multimedia storages holding customer data, and the overall negligence to uphold a security standard for the maintenance, disposal and security of the sensible Data they hold. Article 7[1] precludes the company about using the customer details without their consent for other reasons other than maintain the service the consumer has consented to. The company still uses this material for targeted advertising for this user, of which, is presupposed consent has not been given. Secondly, we are facing the personal data-breaches done by the company, of which we know that the company is not bothered by the event, as they claim, “nobody would know what to do with that data”. As article 83, unreported data breaches to the commission are severely punished by monetary fines that can reach 10 million Euro or the 2% of the global turnover of the company. Lastly but as important, the overall culture of the company regarding the security of the data uphold do not follow the principles of Security imposed by the GDPR commission, therefore making the company completely none-GDPR compliant, which, might face following litigations by the commissions or other third party organization, which would dent the company reputation and financial budget, and, at the worst case, forced bankruptcy of the company itself.

**Summary:**

This report I have managed to nail down the core issues regarding the Cyber security of this **XYZ** company, provided possible solutions following online resources and interviewing professionals that work in the professional industry regarding the topic. Also, I have provided with a list of problems that I think the company would face if the GDPR commission would get involved in an investigation regarding the company.

**Bibliography**

[1]"The principles", *Ico.org.uk*, 2019. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. [Accessed: 18- Nov- 2019].

[2]"Art. 83 GDPR - General conditions for imposing administrative fines - GDPR.eu", *GDPR.eu*, 2019. [Online]. Available: https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/. [Accessed: 18- Nov- 2019].

[3]"Art. 32 GDPR - Security of processing - GDPR.eu", *GDPR.eu*, 2019. [Online]. Available: https://gdpr.eu/article-32-security-of-processing/. [Accessed: 18- Nov- 2019].

[4]"Why GitHub Could Be Your Weakest Link and How to Protect Your Organization | LogicHub®", *Logichub.com*, 2019. [Online]. Available: https://www.logichub.com/blog/why-github-could-be-your-weakest-link-and-how-protect-your-organization. [Accessed: 18- Nov- 2019].

[5]*Us-cert.gov*, 2019. [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/RisksOfPortableDevices.pdf. [Accessed: 18- Nov- 2019].

[6]"Personal data breaches", *Ico.org.uk*, 2019. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/. [Accessed: 18- Nov- 2019].

[7]A. Hern, "Uber fined £385,000 for data breach affecting millions of passengers", *the Guardian*, 2019. [Online]. Available: https://www.theguardian.com/technology/2018/nov/27/uber-fined-385000-for-data-breach-affecting-millions-of-passengers-hacked. [Accessed: 18- Nov- 2019].