1. **Introduction**

Data privacy is the protection of personal information, and data breaches can have serious consequences for individuals and organizations. One notable data privacy incident occurred at Blizzard Entertainment, a leading video game developer and publisher, in 2012.

Activision Blizzard, a video game company, had a security breach on its Battle.net gaming portal where personal data of its users was accessed by attackers. The company reported that no financial information such as credit cards, billing addresses, or real names were compromised. However, information obtained by the attackers included a list of all Battle.net players, except for those in China, along with personal security questions, mobile, and dial-in authentication information of players based on North American Battle.net servers. The passwords of North American server players were also accessed and encrypted using the Secure Remote Password (SRP) protocol.

The company advised all players to change their passwords and update their secret questions and answers, as well as download new authenticator software for mobile authenticator users. The breach may have been carried out for harvesting email addresses for phishing attacks, or for converting virtual items into cash. The exact time of the breach is unknown, and the investigation is still ongoing.

2. THE LEADING FACTORS TO THE BREACH

As the investigation is still underway, the causes of the breach at Blizzard Battle.net are not made public. The following are a few typical reasons for data breaches, according to my training on the OWASP Top-10 privacy risks project:

Apart from general thoughts and the case is still under investigation yet the assumptions are it could be P1 of owasp privacy risk which identifying weaknesses in the web – web application vulnerabilities so this can let the hacker to identify the weakness in the system to exploit and reach the necessary information which exposed the username and passwords

The factors could to these issues also

Weak passwords: If users select passwords that are simple to guess or crack, it may be simpler for attackers to access confidential data.

Inadequate security measures: The danger of a breach increases if the firm does not have suitable security measures in place, such as firewalls, intrusion detection systems, and access controls.

Phishing schemes, email impersonation, and other social engineering techniques can be used to fool people into disclosing their login information or other sensitive data.

Lack of encryption: If hackers obtain access to the data store, sensitive information that is not secured can be easily accessed.

3. Proposed solution

Several recommended practices should be followed to stop data breaches like the one Activision Blizzard faced in the future:

They should have strong principles compliant with GDPR (General Data Protection Regulation) to provide educated control over users and provide strong privacy guideline for providing strong encryption methods of the data in case of any attacks to protect the data

To fix any vulnerabilities, update, and patch software systems often.

Implement effective authentication procedures and access controls, such as multi-factor authentication.

Inform staff members on data privacy and security best practices, such as seeing and reporting questionable activity, on a regular basis.

When storing or moving sensitive data, use encryption.

Conduct frequent security assessments, such as vulnerability scans and penetration tests, to find and fix any potential system flaws.

Keep a disaster recovery plan in place so you can react and recover fast from any security events.

Check logs and network activity often to spot and address any security incidents.

Only those who truly require access should have it.

Organizations can lower the risk of data breaches and secure sensitive information by implementing or following the guideline along with regulation controls