Database Report Results & Security Best Practices

Angela Ruhstorfer

CS-499 – Computer Science Capstone

Southern New Hampshire University

Professor Brooke Goggin

July 31st, 2022

**Report Results**

After creating my animalshelterdb database in MySQL, I wanted to run some statistical data mining reports on its data. Two questions I wanted to confirm, did an animal’s age have an impact on their adoption status? The other being, did having the rabies vaccine affect an animal’s readiness to be adopted?

To confirm the first question regarding age and adoption status, I ran SOFAstats on the ‘age’ and ‘adoption\_status’ columns from ‘animal’ table in my database. To see the full report, please look at the “ageVSadoption - report.pdf” document. This concluded that age did not have an impact, as animals that were both old and young had been adopted.

To confirm the second question regarding having the rabies vaccine and readiness to be adopted, ran SOFAstats on the ‘rabies’ and ‘ready\_to\_adopt’ columns from ‘vet\_report’ table in my database. To see the full report, please look at the “rabiesVSadoption - report.pdf”. This concluded that an animal that did not have the rabies vaccine was not ready to be adopted.

**Database Security and Best Practices**

In today’s age, it is extremely important to secure your technology. Regarding databases, there are multiple ways to keep your databases secure at the physical, network, user, and application levels. We will go over each level below.

Regarding the physical protection of your database server, the server should be secured in a locked and monitored environment, which prevents unauthorized access. It is also best practice to not have the database server hosted on the same machine as your application and web servers. “The backup and recovery procedures are documented and meet data proprietor’s requirements” (Berkeley University of California., n.d.).

For network security, your database server should be behind a strict firewall that only allows traffic to your specified application and web servers. “Firewall rule change control procedures are in place and notification of rule changes are distributed to System Administrators (SAs) and Database Administrators (DBAs)” (Berkeley University of California., n.d.). It is also strongly recommended to regularly test your firewall and other network protections to ensure they are working properly.

User best practices are also important to consider when protecting your database. The user’s workstation needs to meet the security standards of your company to access the database. When stepping away from their workstation, the user should always lock their workstation. “Users are granted the minimal permissions necessary for their job function in the database. Permissions are managed through roles or groups, and not by direct grants to user IDs where possible” (Berkeley University of California., n.d.).

Lastly, there is application security. It is recommended to always keep your programs related to your database up-to-date and upgraded whenever necessary. All components, such as tools, applications, and the servers themselves that have access to the database are documented. “All unused or unnecessary services or functions of the database are removed or turned off” (Berkeley University of California., n.d.).

**References**

Berkeley University of California. (n.d.). *Database Hardening Best Practices | Information Security Office*. UC Berkeley. Retrieved July 31, 2022, from https://security.berkeley.edu/education-awareness/database-hardening-best-practices