Potential Security Threats

# Database Injection Attacks

Database injection attacks are a major threat to database security. They are most often used to attack websites rather than applications using databases. Hackers use malicious code to manipulate the database in the backend and access information that is not intended to be displayed (Rubens, 2018). This may be possible due to inefficient and improper code. For instance, user input fields may unintentionally allow SQL statements to execute and directly query the database (How to Protect Against SQL Injection Attacks, n.d.). If this happens, attackers can gain administrative rights to the database and destroy sensitive company data and private user information. There are two types of database injections: SQL injection attacks and NoSQL injection attacks. SQL injection attacks are oriented towards the traditional database systems where NoSQL injection attacks are targeted towards unstructured data.

One way to address this threat is to examine the input validation before it is processed and ensure that input is of the correct type, length, etc. Another way is to use SQL queries and stored procedures with parameters so that user input will not change the pre-compiled execution plan (How to Prevent SQL Injection Attacks, 2019). A third method is to have a web application firewall that helps filter out harmful data and provide protection from a newly discovered vulnerability until a patch is available to fix the issue (Rubens, 2018). Finally, frequent updates to applications and databases can help patch and repair security flaws and holes that have been discovered.

# Excessive Privileges

Another major threat to database security is excessive privileges. The granting of excessive privileges is the top cause of data breaches. Excessive privileges occur when employees are given access to more of a database system than they need to perform their jobs (Maurer, 2015). When this happens, employees may take advantage of the privileges they have been granted. They can use these privileges to edit data for their own benefit. For example, they could change the amount owed to them in a paycheck. As a result, companies can incur large losses from employees who are given excessive privileges.

There are two methods for dealing with the threat of excessive privileges. The best way to limit the impact of excessive privileges is to monitor what users can access so that any excessive privileges that have been granted can be removed before they are exploited. Therefore, companies should review the access rights of each employee at the company on a daily basis to ensure that they do not have access to more data than they need. The second way to mitigate the threat of excessive privileges is to create views whenever there is a need to give an employee access to certain data. Views will give the user access to the needed data without giving them access to other unnecessary data and help improve security by masking data. Thus, views will allow companies to avoid giving users excessive privileges.

# Human Negligence

Although many of us don’t intend to harm any system that we may be working with, our negligence towards security can compromise database systems. Social engineering is one of the common ways for systems to get compromised. Social engineering is the art of manipulating people to give up confidential information (What is Social Engineering?, n.d.). Attackers take advantage of an individual's trust and mislead them into giving them information that allows them to log in to a system. One way that attackers can accomplish this is by sending an email pretending that they are a trusted person. This email will contain a phishing link that will prompt the user to enter their login information.

Basic bad habits can also be very detrimental to the security for a system. A simple behavior like leaving an unattended computer unlocked is very dangerous as someone can have complete access to the computer. Many people have several different accounts, which makes it nearly impossible to remember all of the different login credentials for those accounts. Therefore, many people write down their username and password on a sticky note (Reinicke, 2018).

These simple actions can be avoided with simple solutions. Having the spam filter set to high and installing anti-virus software are excellent ways to prevent social engineering (What is Social Engineering?, n.d.). In order to easily maintain many log-in credentials, one can use a password manager that will securely store and create passwords.

# References

*How to Prevent SQL Injection Attacks*. (2019, August 2). Retrieved March 29, 2020, from Positive Technologies: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/

*How to Protect Against SQL Injection Attacks*. (n.d.). Retrieved March 29, 2020, from UC Berkeley: https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/how-protect-against-sql

Maurer, R. (2015, July 30). *Top Database Security Threats and How to Mitigate Them*. Retrieved March 29, 2020, from SHRM: https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx

Reinicke, C. (2018, June 21). *The Biggest Cybersecurity Risk to US Businesses is Employee Negligence, Study Says*. Retrieved March 29, 2019, from CNBC: https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html

Rubens, P. (2018, May 2). *How to Prevent SQL Injection Attacks*. Retrieved March 29, 2020, from eSecurity Planet: https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks.html

*SQL (Structured Query Language) Injection*. (n.d.). Retrieved March 29, 2020, from Imperva: https://www.imperva.com/learn/application-security/sql-injection-sqli/

*What is Social Engineering?* (n.d.). Retrieved from Webroot: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering