SECURITY CONTROLS IN SHARED SOURCE REPOSITORIES

FATIH SULJOVIC

CREATING A PROTECTION POLICY

When the team beings building the code they need to know secure coding practices. This should be taught to the team once they are hired to prevent potential data risks that may occur. There is a lot of sensitive data that can be obtained from even a smaller website or application as long as there is a way to input data.

RESTRICT ACCESS TO THE DATABASE

Leaving access only to the direct members working on the project is a good strategy to keeping the database secure. The easiest way to do this is to set up two factor authentication. If the public has access to the database or can find a way in then the data within can be compromised.

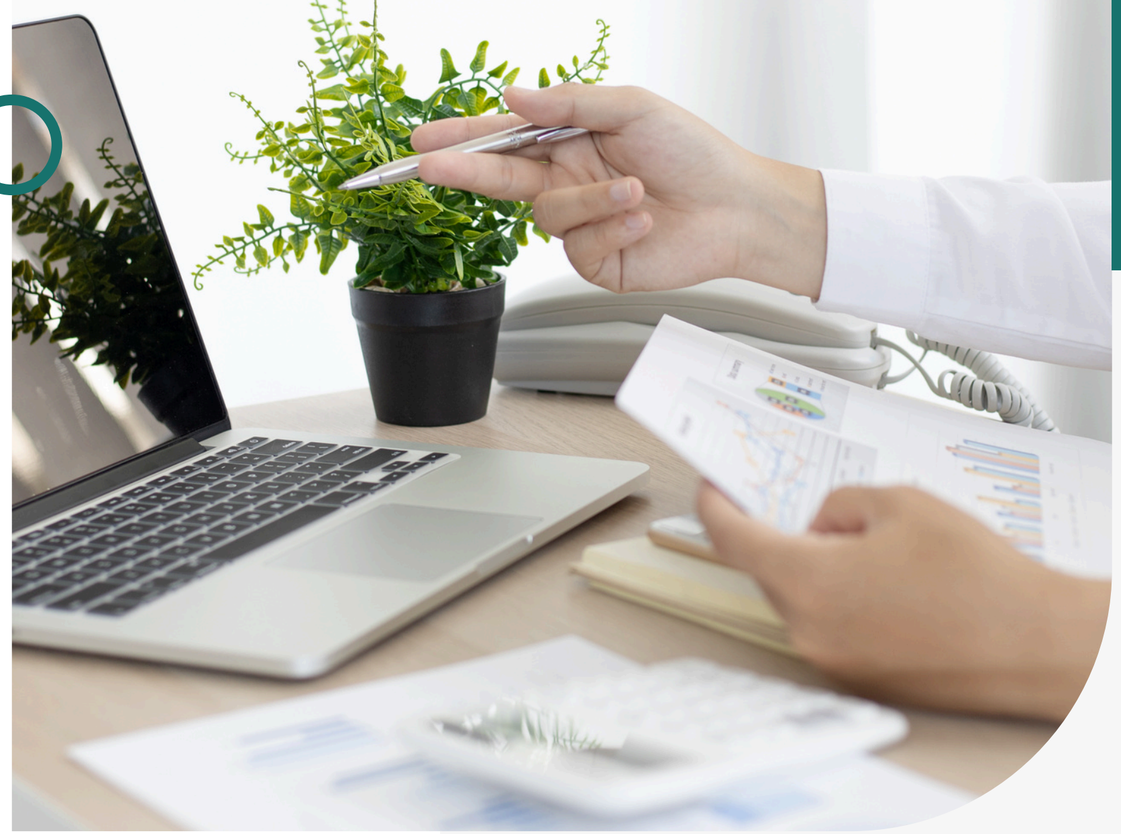
ENCRYPTION

When setting up anything revolving around secure data the best practice is to encrypt that data when its sent over and back from the database. This helps stop the risk of potential hackers catching an individuals key and accessing their data.

NETWORK SECURITY

Adding network security to the arsenal is a great way to layer protection for the customers. Any protection such as a VPN or firewalls can help greatly reduce the chances of individuals data being tracked by hackers.

ENDPOINT SECURITY



Securing the endpoint in the code allows the flow of information to be tracked. Therefore any problems that may arise logs will be taken to ensure action can be had. Preventing the source code leaks from within as well as the previous attempts to protect from outside. Not everyone is going to agree with the current path and potential data can be leaked from a member of the team.

RESOURCES

- BERECKI, B., & BERECKI, B. (2022, JUNE 10). BEST PRACTICES FOR SOURCE CODE SECURITY. ENDPOINT PROTECTOR BLOG. HTTPS://WWW.ENDPOINTPROTECTOR.COM/BLOG/YOUR-ULTIMATE-GUIDE-TO-SOURCE-CODE-PROTECTION/