8-2 Journal

By Thomas Fiske

6/25/2023

It is very important that security is not left until the end of the project and that security is woven into the fabric of the culture of the company. This means that the company should expect to spent as much time/money on security are they do development or testing. The reason for this is because there needs to be adequate security on all systems, and more security on sensitive systems. Having security be a part of the development process and the culture will have the developers thinking with a secure coding mindset which can help eliminate problems from the get-go.

Every security policy will have their pros and cons. It is important to weigh these two categories so that there is a healthy balance. Too much security and a user will probably not use or be able to use your system. Too little security and your data as well as your costumer’s data will be stolen. This all depends on the type of data that is being secured as well. For example, it is very important to keep people financial information secure and it would require more security. Something that is less sensitive can survive with lower security but the balance is what is important.

Zero trust is a good way to be from a security standpoint. I like to think of a system as a room full of files that have sensitive or classified information in. No one is allowed to go into that room without showing their I.D. badge, like a lot of buildings. The same is true of systems. A user should not be able to access sensitive data without proving that they are who they say they are. They need their virtual I.D. badge to access the system in other words.

Implementation and recommendation of security policies again depend heavily on what is being protected. There are baseline things that should be present with every system such as authentication, accounting, and authorization but every system is unique and needs its unique security. One bank will have a different virtual security system than another bank. It is important to take in as much information as possible before making recommendations and the rest of the developers will need to buy into the plan. This means that the implementation needs to make sense and try to avoid creating hardship on certain developers if possible. It is important to hear the developers needs as well and help them secure the system by giving them the tools that they need.