Treyton Davis

CS-405

June 27, 2024

Module Eight Journal

**Adoption of Standards/Not Leaving Security Behind**

Being able to help improve security and ensure security is always being developed beside the main system is an amazing thing to learn. During the time of this class, I have learned many things about secure code and ensuring to never forget about security needing to be built at the same time has helped me learn many things, especially about security vulnerabilities and holes in code.

**Evaluation/Assessment of Risk and Cost Benefit of Mitigation**

Being able to identify risks and finding out the cost to mitigate or fix has also helped me since most of my career will be spent developing code for clients that need the upmost benefit of security to help them feel like they are cared about by the team. Learning about the cost benefits to mitigating risk has been very helpful since some costs can be very small, like assignments in a selection statement instead of comparing two values, or very large, like entire APIs not being secured correctly.

**Zero Trust**

Zero trust is something used at my current job because a lot of the associates working there are field associates either on a salesfloor or backroom. I have come to trust zero trust because I have heard many horror stories about zero trust not being implemented and companies losing millions because someone found a high-level employee’s information that was then used to hack one company. This can easily be avoided by ensuring zero trust is active because it can force a person to verify through an authenticator application to ensure they are who they say they are.

**Implementation/Recommendations of Security Policies**

Throughout the whole course, we learned about security policies and how best to implement the policies across the company. To ensure full compliance with the new policies, monthly meetings would be needed to ensure everyone keeps in mind the new policies for a while, then being able to not have meetings until a new security policy in enacted to keep up with new variations of vulnerabilities and hacking events.