Zaccheus Everett

CS-405

12/22/24

Reflecting on the class, my ideas on adopting a security standard and not leaving security to the end, evaluation and assessment of risk and cost benefit, zero trust, implementation and recommendations of security policies have developed. From the projects I have been given throughout my college education, I had always assumed that security was something left for when the project was mid development. I thought that after the project had a solid foundation and parts of it worked as expected, a security manager object would be coded and attached to the project to meet security standards. I now understand that it is nowhere near that simple. Good security planning is a part of the solid project foundation that makes a good project. Coding standards are a part of the foundation that allows the team to know what their security goals are and just as importantly, stay on the same page. Additionally, I understand that by not leaving security to the end, the project can move along at a healthy pace by avoiding the costly and time-consuming efforts of retrofitting to meet security needs and standards.

For the evaluation of risk and cost benefits, I had to assume that the balance was something that was painstakingly difficult due to how often I see companies who were caught ignoring basic and/or advised security measures. I still think that evaluating is still difficult especially for companies who do not have the funds to spare immediately. With the resources available to the increasing amount of incidents that are appearing, I believe that evaluation and assessment of risk and cost benefits are a part of the initial steps for companies to determine if they are even able to begin doing business in the first place.

Zero trust is something that is easier to wrap my head around. As mentioned in my zero trust discussion post, I believe that in an increasingly online world, not trusting should be the default response. I also believe that coming from a more trusting world into a zero trust one may annoy individuals who were used to freedoms they previously enjoyed. However, much like the famous saying “One bad apple spoils the bunch”, we live in a world with several individuals who would leap at the chance do malicious things if given the chance. Therefore, I feel that now more than ever, in this automated and online world, where anonymity and remote access reign, a zero trust policy is worth the restrictions it comes with much like the how things have changed at the airport.

Finally, for the implementation and recommendation of security policies, I believe that it is important to get everyone on the same page. When from when I started my college education to now, I have only done one group coding project, so I am hardly an expert on how to work with or in a group. However, to me it is this exact lack of group experience that leads me to believe that working together on a project would be very hard. Additionally, security is clearly a more advanced topic considering that this is the only class that has gone through more than a passing glance at it. Implementing proper security policies grant the triple benefit of providing a direction to work towards, getting developers on the same page, and building the solid foundation within the company for security.