8-2 Journal: Portfolio Reflection

Jeremy Depenhart

**Adoption of a secure coding standard, and not leaving security to the end**

In the realm of computer science, there are general standards we abide by to keep our code maintainable, readable, and reliable. This also holds true in secure coding. There are already standards available for adoption that act as a roadmap for you and your organization. Adopting one of these standards will help act as guidelines for you throughout development and ensure that you can easily secure your code from the very beginning. Keeping up with security from the beginning is crucial as it helps avoid the issues and additional costs that come with leaving it until the end.

**Evaluation and assessment of risk and cost benefit of mitigation**

Evaluating and assessing risks is an important step in planning your code with security in mind. It can help you understand what the risks are and allow you to plan to avoid them. From this concept you can mitigate risk and increase benefits of security as much as possible.

**Zero trust**

Zero trust is an important practice in the modern security world. It is the idea of assuming no one is trustworthy by default and instituting checks to help ensure only the right people have access to your network. Accounts can be hacked, and access can be gained by malicious parties. So, it is important to make sure everyone is who they claim to be before providing any level of trust.

**Implementation and recommendations of security policies**

Implementing a security policy will help your organization stay secure. It will give you a base template on how to plan your code and what areas of security to keep in mind. It is important to investigate different policies and narrow down the ones that work best for what you are creating. Then recommend that policy to your organization.