Ashley Santo

Journal: Portfolio Reflection

When a company is creating a policy for developers and other team members to follow, it chooses coding standards based on what fits the company best. Adopting coding standards has multiple benefits such as a more consistent, uniform code base even though it’s written by different developers. This gives the code written more readability and makes it easier to maintain when other developers go in to look at it. It becomes more understandable and increases efficiency of developers. Therefore, not as much time needs to be wasted on deciphering. It also makes it easier to reuse code and detect errors or warning easily. And most of all, it can help keep vulnerabilities from showing up all over the code as long as developers are following the guidelines. This goes hand in hand with the statement “don’t leave security until the end”. It means being proactive with security throughout the entire development lifecycle. It’s important to watch for errors or vulnerabilities when moving through stages and to always have secure coding in mind. Waiting until the end can leave vulnerabilities in the software as well as be more expensive and time-consuming to go back and correcting issues. Security should be built into the software and not just an afterthought at the end. This way, potential problems can be caught and addressed early on.

In most cases, when issues do show up, they go through what’s called a risk assessment to determine what’s the order of correcting the items. First, is determining the overall severity of the vulnerability or how serious will the consequences be if the issue if ignored. Then, there’s determining the likelihood that a vulnerability will be introduced that can then be exploited. Lastly, the cost to correct the issue. Errors with high severity should be handled first because these are things that can lead to dangerous consequences if ignored. It could be data leaks or exploits that could lead to unauthorized users in the source code. After that is determining the likelihood. If something is unlikely to introduce a flaw, then it doesn’t need to have a high priority to correct it. And then cost comes in where if you have two items with equal severity and likelihood, the one with the lower cost would get fixed first because it will be faster and require less resources. There’s a different assessment given depending on each situation.

Zero trust is a security measure that requires all users to be authenticated, authorized and then continuously validated to keep having access to the network. This could be for users or devices inside or outside the network. Just because a device was previously trusted on a network, does not mean the user of the device can be trusted. It also doesn’t mean the device itself is safe. The idea is to constantly validate that the device and user are authorized users that are allowed in the network.

Implementing security policies is crucial to any business because it helps developers follow a set of guidelines that can help prevent or delay attacks. By having security policies in place, the company, employees and users are all being protected whether it’s protecting company or customer information in physical or digital forms. It should never just be the same set of standards every time either. There should be recommendations constantly made to the policy and new standards should be added as they become relevant or the risk of creating a specific vulnerability is higher. Technology is ever-changing and we must keep policies and standards to match the newest potential hazards.

Citations

Kumar Pal, S. (2022). *Coding standards and guidelines*. GeeksforGeeks. Retrieved from <https://www.geeksforgeeks.org/coding-standards-and-guidelines/>

Schiela, R. (Ed.). (2020). *SEI cert C++ coding standard*. Confluence. Retrieved from <https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682>