David Hammons

Southern New Hampshire University

CS-405 Secure Coding

Module 8 Journal

When it comes to secure coding standards the best thing you can do is make sure that you start thinking of it pretty much immediately when you start thinking about the coding process. Having an established security policy from the start helps to ensure that security first practices are being followed from the very beginning. It also helps in creating a clear vision to the team on what they should be doing when they are coding the application like how to validate input, or how to ensure that specific variables are being declared and used properly within the application. It’s not an entirely foolproof plan but it helps to address security from the beginning which makes it much easier in the end when you need to do the final checks and go overs to ensure everything works, is compliant and that there are no vulnerabilities in the code.

Another thing to think about when it comes to secure coding is the evaluation of rish and cost benefits of mitigation. It doesn’t make sense if you have to spend more than what the value of what you are protecting is. So it becomes a balancing act of ensuring that you are cost effective with your security but also making sure it is as secure as you are willing to make it. This does mean that there may be a bit of risk tolerance at play here where you can accept the risk to a certain level if it happens. This can help to get an idea of the security controls and tools you will be using to help with your program from the very start as everything should be done and thought of with a security first mindset in place.

Zero Trust is the idea that everything could be a threat and to always verify anything and everyone before allowing access to the network. This could be done by using certificates, authentication credentials, etc.. Usually there is a Policy Enforcement Point that acts as the stop for all devices trying to get onto the network. The Policy Engine then determines if access can be granted and the Policy Administrator grants the connection to the device based on the decision of the Policy Engine. This helps to prevent threats not just outside of the network but also inside the network as well as those should also be as not trusted as devices on the outside. Zero Trust also uses implicit deny as a way to ensure that nothing unauthorized can gain access to the networks and steal data or wreck havoc in the application.

As such that when it comes to recommendations and implementations you need to from the start look into what you want to have for security, the cost associated with everything and start to establish a baseline on how to go about with implementing security into your code. This is a sure way to ensure an easier process overall and that everyone on the team is on the same page when it comes to security and being consistent with their code and consistency with their security mindset as well.