Merlin Martinez

Module 8.2

08/19/2024

Journal

This class has provided me a very clear understanding of security like for example security protocols, and secure coding, all these tools that where provided to us in this class gave us a good insight on how to mitigate possible vulnerabilities, it thought us what not to do and how we have to make sure from the very beginning to not leave your security for the end, to start from the beginning from the design phase because if you do so the security can go through the necessary testing phases in order to help lower the risks of attacks, in addition this class thought us that the system security; when is left for last can become compromised and it can make the system more vulnerable to attacks making the users and the company involve in data and even in a financial loss. Whenever we talk about not leaving security to the end we talk about how important it is to start early even after the program has been started this means you are going to have more work however is never too late this means that the process is more difficult as there will be many areas to unpack and maybe even a lot of back tracking, this takes more time and money.

The risk and cost benefit of mitigating helps to show how the risks, costs, and benefits of adopting a particular practice or standard. In our project we did a table showing the risk, levels, cost, severity etc. this helps to show and determine what’s the priority. By doing good coding stand and implementing the right security this can help with limiting the risk and big costs.

Zero trust or no one is safe is a good standard to employ. This means you are not taking any chances by implementing secure coding protocols like for example AAA framework or encryption can help to lower the risks of any hacks. Whenever we implement zero trust, or no one is safe we meant we must verify and authenticate before anything. Whenever passing information between computers even if using the same network, it should always be encrypted, another good approach when sharing sensible information would be encryption at rest, encryption in flight and encryption in use.

In conclusion I would recommend using a good secure, organized, clear and simple format. Adopting DevSecOps security standards and practices throughout a development cycle.

Resources

AWS. What is DevSecOps? <https://aws.amazon.com/what-is/devsecops/>

Microsoft. What is DevSecOps? <https://www.microsoft.com/en-us/security/business/security-101/what-is-devsecops>

Fortinet. What is Authentication, Authorization, and Accounting (AAA) Security? <https://www.fortinet.com/resources/cyberglossary/aaa-security#:~:text=Authentication%2C%20authorization%2C%20and%20accounting%20(AAA)%20is%20a%20security,enforces%20policies%2C%20and%20audits%20usage>.