Spencer Erickson

8-2 Journal

12/18/2022

Adopting a security code standard allows for consistencies to be developed and a robust well-planned security protocol to be set in place. A strong and consistent security standard Will effectively protect a system from threats of all kinds. The "Do not leave security to the end" practice simply implies not putting developing security measures near the end of the project's development. Waiting till project completion to develop security protocols can lead to vulnerable unreliable code susceptible to attack.

It is essential to devise a plan and evaluate your project to access the most effective security protocol, both functionally and financially. Your budget will dictate how in-depth your defense systems can be. There is a time and place for everything; not all systems require extreme security measures, while others do. By defining our threats and describing them in the security protocol, we could better defend ourselves from attack and ensure we were allocating funds to the needed security to protect us from said attackers. Teams can manage their time to correct and develop defenses against these specific threats to protect the project from attackers.

The zero-trust policies have been implemented in many government databases. Zero-trust policies are being implemented into systems and databases for civilian corporations and individual accounts to protect the funds and security of the data. These types of policies request triple-A policies and encryptions to be accessed for even employees to view the data. This defense not only protects the companies from attackers on the outside, but it protects them from even potential insider threats by incorporating securities policies that are very in-depth.

As hackers' attacks continue to evolve, so must our security policies. By ensuring that we can continuously adapt to new strategies and implement changes along the way, we allow ourselves to protect our programs and systems better as new attacks develop.