Kao Chao

12/13/2022

CS-405 Secure Coding

8-2 Journal: Portfolio Reflection

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

Every development team should adhere to secure coding standards. Even the most experienced

programmer can make a coding mistake unintentionally. And even one mistake can set off a

minor hitch. A serious security breach would be considerably worse. Secure coding stops private

data and business information from leaking into the public domain. Credentials such as

passwords, API keys, tokens, etc. We can clarify that when implementing any infrastructure or

solution, security should be one of the top considerations. Getting rid of the attack surface is one

of the fundamental principles of protection. Although incorporating a security-by-design

the approach to projects may seem like a bother for organizations, but it may save time, money,

and effort in the long run. Organizations that fail to think about security from the start are

frequently easy targets for hackers. The method can be made as complicated or straightforward

as you wish, but the effort is worthwhile. The important thing is that you're thinking about

project security as early as feasible and, as a result, producing a more secure product.

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

With the gradual mainstreaming of newer technologies like cryptocurrencies, the Internet of

Things (IoT), and artificial intelligence/machine learning (AI/ML), have weaknesses,

And there are more security threats to be concerned about. The inherent trade-off between

paying to prevent a disaster from occurring versus paying to clean up a mess is one of the most

crucial points to emphasize in your CBA (Cost-benefit analysis). Naturally, spending money on

preventative cyber security measures has a price. Given that spending varies from company to

company and industry to industry, there is no accurate way to calculate an “average" cyber

security budget. The expense of prevention is usually negligible in relation to the expense of a

breach.

* Zero trust

A security framework known as "Zero Trust" mandates that all users, whether inside or outside

the organization's network must first be verified, authorized, and continually checked for

security configuration and posture before access to applications and data is provided or

maintained.

* Implementation and recommendations of security policies

Implementing the Policy –

Check the status of compliance If your system doesn't adhere to your policy, you might need to

make changes to it. Run a compliance check after applying patches or updates if you'd like.

Make concise, insightful policy statements. Determine which systems need to be connected to

the controlling system and which contain important data. Add these devices to the system

configuration list in Secure Perspective.

Recommendations Policy –

Cover all organization-wide security procedures from beginning to conclusion. Be consistently

updated to reflect changing business requirements and security concerns.

References:

10 Absolute Best Ways to Mitigate Security Risk

Posted on January 19, 2022 by [Marho Atumu](https://www.liquidweb.com/blog/author/matumu/) | Updated: February 10, 2022

**A Cost-Benefit Analysis Approach to Cyber Security**

By: [Toby Shackleton](https://www.6dg.co.uk/author/toby-shackleton/)  [March 3, 2021](https://www.6dg.co.uk/2021/03/03/)