**8-1 Journal: Reflection**

Dylan Jeffery

SNHU

CS-405

Trevor Hodde

12/16/2021

For this reflection we were asked to examine and discuss a few topics regarding the implementation of our security policy, and the thought process behind some of our choices. The first topic being adopting a secure coding standard and not leaving security to the end. We cannot ever just assume that any attack vector won’t be attempted to be exploited. We must consider that anyone could do anything to try to gain access to our system, and we must account for this. The truth of the matter is that we have to design around the assumption that somebody with unlimited time and resources is out to get us, and we must do everything we can to ensure all our ‘doors’ are locked. This comes from test-driven design and using secure network practices. The rest is maintaining and regularly updating our software as well as our policies.

Regarding evaluation and assessment of risk/cost benefit analysis there are a few important considerations as well. Risk evaluation is where we consider the seriousness of a particular risk in relation to other risks. Assessment is a process of identifying hazards and potential vulnerabilities within a company and implementing appropriate safeguards and strategies in a way that minimizes the exploitability of our systems. Mitigation has to do with configuring and maintaining our security procedures, whether it is through network security like firewalls and using secure repositories or through sticking to our established security policy.

The basis of a ‘zero-trust’ policy relies on not trusting anything inside or outside organizations and relying on verification of connections before granting access. Zero trust revolves around authentication, authorization, and validations. These are often based on real-time visibility in user attributes like...

User ID

Firmware version

Endpoint hardware type

OS version

Patch level

Vulnerabilities

User logins

Application installed

Security/incident detections

For us, a policy of zero trust includes:

Using multifactor authentication to validate and secure identities.

Managing and validating that devices are healthy

Using a policy of providing least privilege.

Through zero trust segmentation, we can create boundaries between regulated and unregulated data, further protecting our sensitive data.

Finally, security policies outline recommendations that when followed can help protect our organization and data. A lot of consideration goes into quantifying threats that an organization may face, and the standards outlined in a policy are carefully chosen for the widest case variety that we may face. The most important benefit is simply that security policies allow our developers to all be on the same page, creating test-driven secure software.