Diego Bez Zambiazzi

August 19, 2021

8-2 Journal: Portfolio Reflection

CS-405

The adoption of secure coding standards, such as CERT, CWE, OWASP, is crucial to developing secure applications. These rules and guidelines define practices, methods, and style that mitigate software vulnerabilities. Furthermore, automation tools, such as Static Application Security Testing, can be used to verify if coding standards are being followed and identify vulnerabilities in the code. This is one example of how to approach development taking security into consideration instead of leaving security to the end. Following a DevSecOps process ensures that security is evaluated in each step of the development lifecycle, from planning to threat response. With automation, this can be done in pre-production by using threat modeling, unit testing, mocking, compile build checks, and static application security testing, and in production by running deployment health checks, runtime application self-protection, and automated incident response.

Mitigating risks and vulnerabilities comes at a cost, as it can require investments in resources such as hardware, software, processes, training, and staffing. Since it is not possible to attain a system that is completely secure, organizations should create threat models to identify and focus on specific priorities. For instance, small companies have a threat landscape that differs from that of banking or governmental institutions. Balancing tradeoffs is crucial in defining the optimal investment in security strategies for each scenario. This is particularly important when implementing a defense-in-depth strategy that is built on multiple layers of technical, administrative, and physical controls.

A security concept that emerged from recent changes in business needs is the concept of a zero-trust security model. With employees accessing sensitive data from different locations and devices, the security perimeter is not limited to the company’s network anymore. Zero trust shifts the focus to verifying device, user, transport/session, application, and data trust. According to Scott Matteson's article "How to prevent ransomware attacks with a zero-trust security model," following the principle of "never trust, always verify" could have avoided recent ransomware attacks suffered by Colonial Pipelines, JBS, and Brenntag. Changing the focus of security from the network perimeter to a combination of verification and permission policies based on device, user, transport/session, application, and data trust makes it much more difficult for attackers to succeed.

Lastly, implementing security policies is also an essential part of cybersecurity. For instance, policies can define when and how data should be protected with the use of encryption. Furthermore, policies can enforce the concept of Triple A and determine details regarding user authentication, authorization, and accounting. These policies ensure that secure practices are followed, allowing for a consistent code and efficient collaboration. Furthermore, policies and standards should be linked to security principles, such as default deny and architect and design for security policies, to establish a cohesive security strategy.

References

Kueh, T. (2020, Jan 15). A Practical Guide to Zero-Trust Security. *Threat Post*. Retrieved from https://threatpost.com/practical-guide-zero-trust-security/151912/

Matteson, S. (2021, Jul 9). How to prevent ransomware attacks with a zero-trust security model. *TechRepublic*. Retrieved from https://www.techrepublic.com/article/how-to-prevent-ransomware-attacks-with-a-zero-trust-security-model/

Rosenquist, M. (2014, Mar 12). Security is About Balancing Tradeoffs. *Intel*. Retrieved on July 9, 2021, from https://itpeernetwork.intel.com/security-is-about-balancing-tradeoffs/

Start With Security: A Guide for Business. (2015, June). *Federal Trade Commission*. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

Update: Security Notification - March 2021. (2021, Mar 26). *ParkMobile*. Retrieved from https://support.parkmobile.io/hc/en-us/articles/360058639032-Update-Security-Notification-March-2021