SECURITY CONTROLS IN SHARED SOURCE CODE REPOSITORIES

Jacob Ambrose

CSD 380: DevOps
10/05/2024
Module 11 assignment 02

TABLE OF CONTENTS

01 Code Repositories

02 Controls Overview

03 Policies

04 People

05 Software

06 Hardware

07 Conclusion

08 Works Cited

CODE REPOSITORIES

Code repositories act as an all access journal that organizations can use to maintain and share their code.

These repositories also act as version control, allowing organizations to roll back versions as needed and to slowly implement new features.

As these repositories allow access to organizations code, it is important to ensure that best practices are followed to ensure they are secure.

SECURITY CONTROL OVERVIEW

There are various ways companies can work to secure their code repositories. These roughly can fall into four different approaches.

Policies: Internal and external organizational policies such as an incident response plan.

People: These can be the NDAs or other legal agreements with staff.

Software: Restricting access controls.

Hardware Offsite backups and secure endpoint devices assist .

POLICIES

Internal and external Policies can be applied to assist in ensuring code repositories are as secure as possible.

Some examples can be internal policies such as threat modeling, and incident response procedures. It is important to note that these policies should reflect local regulations and be updated frequently.

PEOPLE

The human element of software development cannot be overstated. Maintaining policies to assist in ensuring that the human element does not fail intentionally or unintentionally.

To help mitigate the human element, legal agreements between employees and contractors such as NDAs can be used. These help mitigate any proprietary information being shared.

SOFTWARE

Various software systems can be implemented to help secure code repositories.

Implementing access control such as pull requests so that new code that is not reviewed is pushed into the production branch.
Encryption such as code signing or obfuscation of confidential information such as API keys or passwords are a must. Once an API key is on the internet or password, then everyone will have access to that API or password, necessitating a change across the entire application everywhere.
Additionally, choosing a secure repository software such as Git is a must.

Continuous monitoring upon the repository for any pull requests, changes, or other items can help alert the appropriate parties when changes are made.

HARDWARE

One of the last items organizations can work to make their repositories as secure as possible is ensuring the hardware is secure.

Ensuring endpoint devices that developers use to access the source are secure and trusted.

Maintaining multiple off-site backups of software is a must. Whether that is on various cloud services or an off-site data center is dependent on the organization and their policies.

CONCLUSION

There are many different approaches to ensuring that an organization’s software repository is kept as secure as possible.

It is important to remember that not one of the past approaches is a standalone item. Each and every single one is needed to ensure that the code is secure. By maintaining vigilance and reviewing the internal and external sources of the repository, organizations can mitigate direct threats to the source code.

WORKS CITED

01 Berecki, B. (2022, June 10). Best practices for source code security. Endpoint Protector Blog. https://www.endpointprotector.com/blog/your-ultimate-guide-to-source-code-protection/

02 Brook, C. (2024, May 2). Source code security best practices to protect against theft. Digital Guardian. https://www.digitalguardian.com/blog/source-code-security-best-practices-protect-against-theft

03 Fernandes, C. (2024, March 18). Source code security best practices: A complete guide - blog. Assembla. https://get.assembla.com/blog/source-code-security/

04 Protect your code repository. NCSC. (n.d.). https://www.ncsc.gov.uk/collection/developers-collection/principles/protect-your-code-repository

05 Securing source code in repositories is essential: How to get started. Snyk. (2023, November 16). https://snyk.io/learn/securing-source-code-repositories/