


Security Controls: Source Code

By: John A Garcia III

Professor: Sue Sampson

Assignment #: 11.2

Date: 07/21/2024



Shared Source Code Repository

- Shared source code repositories are centralized locations where code is stored, managed, and versioned, allowing multiple developers to collaborate on the same project
- Version Controls
 - Allow for history of changes
 - Track who makes a revision
 - Allows for branches to be created
- Common shared source code repository tools:
 - GitHub
 - GitLab

Security Importance

- Shared repositories are great for centralizing all changes and collaborating with team members.
- Shared repositories being centralizing all code means that the codebase is vulnerable if there are any open security threats.

Potential Risks

- Unauthorized access (Berecki, 2022)
- Code tampering (authorized or unauthorized access)(Berecki, 2022)
- Data breaches (Berecki, 2022)
- Potential loss of intellectual property; meaning that you no longer own the rights to YOUR codebase (Berecki, 2022)

Mitigating Risks

- Source code protection policy
- Access controls
- Encryption and monitoring
- Security tools
 - Including “Endpoint security”

Protection Policy & Access Controls

- Source Code Protection Policy:
 - This is a policy that should be created to protect code by:
 - Defining protection rules for code interaction (Berecki, 2022)
 - Defining requirements for code interaction (Berecki, 2022)
 - Defining procedures for code interaction (Berecki, 2022)
- Access Control :
 - This means that the only people who have access to the code actually need to have access (Berecki, 2022)
 - This ensures that only certified people are interacting with the codebase repository
 - This may also include having a multi-factor authentication method for those who are certified

Encryption monitoring & Security tools

- Encryption should be used when transmitting or receiving data to/from the codebase repository (Berecki, 2022)
- All data transmissions should be monitored (Berecki, 2022)
 - This may also include white-listing or black-listing specific IP addresses when interacting with the codebase repository
- Security tools that are used often to limit potential unwanted access:
 - Firewalls (Berecki, 2022)
 - Virtual private networks (Berecki, 2022)
 - Anti-virus & Anti-malware (Berecki, 2022)
- Endpoint Security includes the protection of physical employee devices through the use of endpoint security software that will not allow unauthorized code exfiltration (Berecki, 2022)



EndpointProtector.com

Resources

- 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/>