SECURITY CONTROLS IN SHARED SOURCE CODE REPOSITORIES

PAUL ROMER

CSD380

MODULE 11.2 ASSIGNMENT

WHY SECURE SOURCE CODE REPOSITORIES?

- REPOSITORIES CAN CONTAIN INTELLECTUAL PROPERTY, SENSITIVE APPLICATION CODE, SOURCE CODE, AND CONFIGURATION SCRIPTS.
- WORKING IN TEAMS INCREASES THE ATTACK SURFACE WITH EACH PERSON GIVEN ACCESS TO A SHARED REPOSITORY.
- MAKE SECURITY A SHARED RESPONSIBILITY, NOT A BOTTLENECK.

KEY THREATS (CIA TRIAD) :

- CONFIDENTIALITY: PREVENTING UNAUTHORIZED ACCESS TO CODE AND SECRETS.
- INTEGRITY: ENSURING CODE IS ACCURATE AND UNTAMPERED.
- AVAILABILITY: GUARANTEEING ACCESS FOR AUTHORIZED USERS AND SYSTEMS.

AUTHENTICATION & AUTHORIZATION

- MULTI-FACTOR AUTHENTICATION (MFA)
    - MANDATORY FOR ALL USERS.
- ROLE-BASED ACCESS CONTROL (RBAC)
    - ASSIGN PERMISSIONS BASED ON ROLES (DEVELOPER, TESTER, ADMIN) FOR CONSISTENCY AND EASIER MANAGEMENT.
- PRINCIPLE OF LEAST PRIVILEGE (POLP)
    - GRANT ONLY MINIMUM NECESSARY PERMISSIONS FOR THE SHORTEST REQUIRED TIME.
    - REGULARLY REVIEW AND REVOKE EXCESSIVE RIGHTS.

SECRETS MANAGEMENT

- KEEP CREDENTIALS OUT OF CODE.
- NEVER HARDCODE API KEYS, PASSWORDS, OR TOKENS IN CODE, CONFIG FILES, OR COMMIT HISTORY.
- USE AUTOMATED SCANNING.
- KEEP SECRETS IN A CENTRALIZED VAULTS.
- HAVE PLANS FOR INCIDENT RESPONSE.

CODE REVIEW

- REQUIRE PULL REQUESTS FOR ALL CRITICAL BRANCHES.
- REQUIRE REVIEW AND APPROVALS.
- AUTOMATE RULE ENFORCEMENT.
- MAKE ROLLBACKS EASY.

AUTOMATED SECURITY TESTING CI/CD

- AUTOMATICALLY ENFORCE POLICIES.
- STATIC AND DYNAMIC ANALYSIS.
- DEPENDENCY SCANNING.
- CODE SIGNING.

MONITORING, LOGGING, AND INCIDENT RESPONSE

- COMPREHENSIVE AUDIT TRAILS:
  - LOG ALL SIGNIFICANT ACTIVITIES: ACCESS, CODE CHANGES, BRANCH OPERATIONS, PRS, SETTING CHANGES, USER ACTIONS.
- CONTINUOUS MONITORING FOR ANOMALIES:
  - ESTABLISH BASELINES AND ALERT ON DEVIATIONS.
- INCIDENT RESPONSE PLAN:
  - WELL DOCUMENTED, TESTED PLANS.
  - PHASES: PREPARATION, DETECTION & ANALYSIS, CONTAINMENT, ERADICATION & RECOVERY, POST-INCIDENT ACTIVITY.

SOURCES

- HTTPS://WWW.NCSC.GOV.UK/COLLECTION/DEVELOPERS-COLLECTION/PRINCIPLES/PROTECT-YOUR-CODE-REPOSITORY
- HTTPS://SNYK.IO/ARTICLES/SECURING-SOURCE-CODE-REPOSITORIES/
- HTTPS://GET.ASSEMBLA.COM/BLOG/SOURCE-CODE-SECURITY/