2022

Building an Application Security Program

A HIGH-LEVEL APPROACH

SUNIL VARKEY

Overview

Exploits of vulnerabilities or misconfigurations in web applications are one of the primary targets in most recent cyber incidents.

A potential root cause of this is that,

- Applications are built with minimum security considerations.
- Too many changes by different groups impact the overall security
- Federated application management with 'assumed' accountability
- Reuse of codes from untrusted or public domains
- Lack of security assessment before production release or when external/internal environment changes in production
- Lack of security baseline, standard or framework to adhere
- The assumption that 'all is well'

Considering the turbulence, many organizations are in the process of revamping their application security program from the traditional compliance-triggered application security assessment approach: which NOT efficient in the current era.

An effective and comprehensive Application Security program considers

- both the pre-production and production environment,
- looking at the entire lifecycle
  - requirement,
  - design,
  - development,
  - deployment (pre-production)
  - runtime production environment)
- Hosted and dependent environment

Maturity of the program and resiliency of the application over time, based on the availability of resources and capability.

Proposed steps in building an Application Security Program

- **Define the need for security assessments**

  - Risk,
  - Need,
  - Commitment

from the perspective of

  - Business
  - Regulatory
  - Availability
  - Security
  - Privacy
  - Standards and best practices
  - Threat environment
  - Reduction of attack surface
  - Compliance

- **Define Assessment coverage scope and components**

  - Threat Modelling
  - Architecture
  - Software
  - Infrastructure
  - Network
  - Mobile Apps
  - Free and Open source, Layered Software, Binary
  - Containers, APIs
  - Cloud, VM Workloads
  - Databases
  - Authentication and Authorization Rules

Accuracy and completeness of inventory are critical to the success of the program.

- **Application in Scope for assessments**

  - All systems
  - Critical, Internet-facing, Regulatory services
  - SOX / PII / PHI
  - Managed systems
  - Hosted internally / Hosted by 3rd party
  - All customer-facing
  - IT only / IT, OT, IoMT and IoT
  - COTS / In-house
  - Cloud workloads – Pets / Cattle

- **Depth of assessment**

    - Authenticated / Unauthenticated
    - Passive / Active

- **Types of assessment**

    - Vulnerability assessments
    - Configuration assessments
    - Compliance assurance
    - Attack surface assessments
    - Risk assessment
    - Posture assessment
    - Penetration testing

- **Frequency of assessment**

    - Biweekly, Monthly, Annually
    - Every change
        - Minor
        - Major
    - Prior to certification or audits for compliance
    - With new vulnerability disclosures, patch release
    - Changed threat landscape or hosting environment

- **Foundational Policies and Standards** (to be developed or modified based on inputs from earlier points)

    - Security Standards
    - Security Principles
    - Security control Requirements
    - Secure Design solution Security Architecture
    - Secure Dev Standards,
    - Secure Coding Practice
    - Secure Deployment Standard
    - Inventory – Infra, OT, Digital Footprint, Applications
    - Roles and Responsibilities of the stakeholders
    - Lifecycle management
    - RACI matrix
    - Secure software maintenance
    - Control requirement
    - Triage of Vulnerabilities
    - Threshold enforcements
    - Change management – production release
    - Vulnerability Alerting and reporting
    - Remediation strategy

- **Tools & Technology stack (based on scope and coverage)**

  - Static Application Security Testing - SAST
  - Dynamic Application Security Testing – DAST
  - Interactive Application Security Testing – IAST
  - Mobile Application Security Testing - MAST
  - Free and open-source software – FOSS
  - Software Composition Analysis - SCA
  - Infrastructure Security Assessments
  - Container Security Assessments
  - Binary Code Assessments
  - Layered software
  - Threat Modelling
  - Digital foot printing
  - Vulnerability Aggregation Correlation platform
  - Software bill-of-material repository

- **Reporting**

  - Governance and reporting model
  - Aggregation and Correlation – technology, approach
  - Vulnerability classification and criticality definitions
  - Alerting frequency and thresholds
  - Build Authoritative source for configuration and vulnerabilities – Visibility
  - Methods of alerting, reporting, and acknowledgement of issues
  - RACI for risk notification, validation, remediation, acceptance
  - Risk scoring report
  - Metrics
    - Activities
    - Exposure
    - Risk: mitigation, acceptance
    - Non-compliance

- **Program Team and Skills**

  - Threat modellers
  - Penetration Testers – Web, Application, Mobile, Infrastructure, Cloud
  - Vulnerability Assessors – Infrastructure, OT
  - Vulnerability Analysts, Researchers
  - Vulnerability Engineering – development of abstraction layers, integration of tools, maintenance of assessment tools
  - Digital Footprint analysts
  - Visualization, metrics, Dashboard developers
  - Champions: developers, admins (IT, cloud)

- **Execution and Operations (**in phases based on the maturity of the program)
  - **Outsource:** no skills, resources, or tools available inhouse
    - Consultants working from the local network
    - Expose possible applications for remote assessments
  - **Service-based contract –** per application or IP
  - **Hybrid model** – a combination of in-house and outsourced
    - Based on the criticality of applications/systems in scope
    - Assessment tools or services available inhouse
    - Use external service only for regulatory-mandated independent validations
    - Annual Assurance only
  - **Inhouse assessments**
    - Capacity, tools, skills available in-house and workload available for optimal utilization of resources
    - Leverage external capacity only for capacity fulfilment
  - **Shift-Left**
    - Threat modelling - Assessments of security considerations by solution architects at the pre-build stage.
    - Assessment Tools integrated into the development pipeline in-house
    - Automation and tools Abstraction layers (for more straightforward tools adoption) build
    - Workflow functional for assessment, remediation, and production release
    - Shift left capable SAAS platform available to leverage

Remediation

- IT service asset owners/technology SME are accountable for remediating identified vulnerabilities and ensuring configuration compliance.
- Remediation can be done as centralized activity (ex., Microsoft patch across IT estate) or federated based on region/business or service.
- The Security Assessment team provides visibility, priority, and actionable input for asset remediation owners for remediation action.