Network Security Subcommittee Report

F2F 49 Bratislava - 2020-02-19

Overview of Activities

- Three Main Efforts
  - Pain Points (CAs and Auditors) [short/medium term]
  - Threat Modelling [medium/long term]
  - Document Restructuring [long term]
- Suspended “Authentication and Access Control” team - lack of resources.
- General updates to NCSSR document to correct inaccuracies
- Goal remains a series of ballots designed to make the NCSSR (NSRs):
  - more suitable to current security threat landscape
  - easier to derive auditable criteria

Identified Pain Points - 1

- NSR language is too prescriptive
  - Authentication language around password length, lockouts, etc.
  - Heavily influenced by “zones” as a security primitive
- NSR language is too vague
  - Unclear on the application to offline CAs
- NSR text is overlapping/redundant
  - Different “System” definitions mean that a component can fall into multiple categories with overlapping compliance criteria

Identified Pain Points - 2

- NSRs allow reliance on manual review processes
  - Automatic systems more likely to be reliable
- Log retention periods too long
  - 7 years for everything is not typical
- Timing requirements for remediation not clear
  - E.g. 96 hour time to remediate critical vulnerabilities from discovery
    - When does the clock start?
      - From vulnerability scan discovery?
      - From CA's scanning of the results?

Pain Points Ballots - 1

Ballot	Title	Purpose	Status
SC21	Log Integrity Controls	• Add continuous automated monitoring for integrity of logging processes • Extend monitoring to log archival and retention	passed
SC20	Configuration Management	• introduces requirement to control system changes through a change management process. • extends configuration monitoring to all security relevant CA systems • Replaces human review with continuous monitoring to reduce alert response time to (24) hours	discussion
SCXX	Logging and Log Retention	• Reduce log retention period for non-issuance data from seven years to two years	nearly done

Pain Points Ballots - 2

Ballot	Title	Purpose	Status
SCXY	System Account Management	• Adds continuous monitoring for systems accounts on CA systems	preparation
SCYY	Timing Requirements	• Tighten text around remediation of critical vulnerabilities	preparation

Threat Modelling

State of play in Q1 2020

- Threat Analysis underway

Threat Modelling - Activity

- 3 tested methodologies
- 5 Diagrams (4 Data Flow Diagrams and 1 Process Flow Diagram)
- 15 main components of CA systems (after “decomposition”)
- 17 use-cases
- 9 general risks
- All NSRs analysed
- 1 checklist - 30 items

Threat Modelling - Next Steps

- Discuss and evaluate “NSR Checklist” in NetSec Subcommittee
- Analyse use-cases
- Identify threats and risks
- Build new checklists
- Provide ballots for NSR based on findings

Document Structuring

- Looking to make NSRs have a more logical structure
  - Considered renumbering sections to be more like BRs/RFC 3647
  - Considering using Two-Letter Abbreviations (like NIST Cybersecurity Framework)
    - Functions: ID=Identify, PR=Protect, DE=Detect, RE=Respond
    - Categories: ID.AM=Asset Management, PR.DS=Data Security, etc.
- Examining well-known frameworks to inform newer structure
  - WebTrust and ETSI (e.g. ETSI TR 103 305-1, etc.)
  - CIS Controls
  - Others (NIST, ISO 27001, PCI, Cloud Security Alliance, etc.)

Other Matters

- CVSS Ballot
  - correcting out-of-date text regarding CVSS “Critical Vulnerabilities”
  - Ballot nearly ready, just awaiting seconders
- Ensuring a slightly more formal structure
  - Agenda
  - Minutes
  - Ballots to link to discussion documents regarding thought processes
  - Wiki Information for team/subteams
  - Netsec-management list for non-archived mailings