National Cybersecurity Center of Excellence

Data Integrity Project

Recovering from a Destructive Malware Attack

National Data Integrity Conference
3 Jun 16

(Don Tobin, donald.tobin@nist.gov, @don_belowradar)

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

ENGAGEMENT & BUSINESS MODEL

 DEFINE + ARTICULATE Describe the business problem	Define business problems and project descriptions, refine into a specific use case
 ORGANIZE + ENGAGE Partner with innovators	Collaborate with partners from industry, government, academia and the IT community on reference design
 IMPLEMENT + TEST Build a usable reference design	Practical, usable, repeatable reference design that addresses the business problem
 TRANSFER + LEARN Guide users to stronger cybersecurity	Set of all material necessary to implement and easily adopt the reference design

Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards

Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

Organizations:

- store all kinds of data, much of which is essential for their functioning
- face ransomware, destructive malware, malicious insider activity, and honest errors
- need to reduce risk by being able to quickly detect alterations, recover from an attack, and trust the accuracy of the recovered data

Data at risk:

- Current data (transactional data, email, customer PII, employee PII)
- Backup data
- Baseline operating systems and system configurations
- Installed application software

Scenario 1: Ransomware:

Watering hole or drive-by attack: malware encrypts files and displays notice demanding payment for decryption

Scenario 2: Data Destruction:

Spear-phishing campaign with link/attachment: malware destroys data on user and back end systems

Scenario 3: Data Manipulation:

Credentialed employee intentionally or accidentally manipulates data in a seemingly legitimate way

Effectively recover data at risk

Confidently identify:

- Altered data and time/date of alteration
- Impact of the data alteration
- Correct backup version for system and data restoral

Desired requirements:

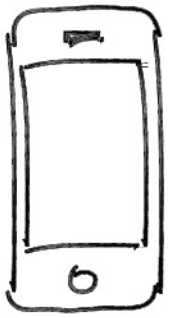
- Automated data corruption testing, data corruption detection, and data corruption event logging
- Detection and reporting of all file and database modifications, deletions, and creations
- User activity recording and correlation of file changes and users
- Anomalous configuration management and user activity detection

Primary business benefits:

- Reducing the impact of a data corruption attack
- Reducing downtime caused by data corruption
- Detecting backup data tampering
- Reducing the negative impact to the reputation of an organization due to data corruption events

Other business benefits:

- Improving IT resource efficiency and recovery speed through automation
- Improving trustworthiness of backup data
- Improving continuity of operations

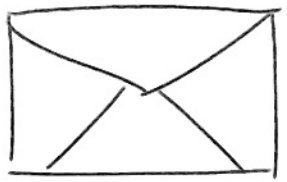


301-928-6667

donald.tobin@nist.gov

Participate

http://nccoe.nist.gov



9700 Great Seneca Hwy
Rockville, MD 20850