BUILDING BLOCK

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DATA INTEGRITY

Recovering from Ransomware and Other Destructive Events

The National Cybersecurity Center of Excellence (NCCoE) is helping enterprises ensure the integrity of their data through collaborative efforts with industry and the Information Technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the project description, *Data Integrity: Recovering from Ransomware and Other Destructive Events*, including background and challenge, goals, and proposed solution. The proposed data integrity solution is not meant to be authoritative; there may be other solutions in this fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or suggest products that might be applicable to the challenge of maintaining data integrity, please contact us at di-nccoe@nist.gov.

BACKGROUND

Businesses face a near-constant threat of destructive malware, ransomware, and malicious insider activities that can alter or destroy critical data. Even honest mistakes can alter data in ways that could cause a significant loss to a company's reputation, business operations, and bottom line. To reduce this risk, organizations need to be able to recover quickly from a data integrity attack and trust the accuracy and precision of the recovered data.

CHALLENGE

Ransomware and other destructive events are decidedly on the rise. According to the FBI, ransomware payments are expected to cost companies $1 billion in 2016, compared with $24M spent in all of 2015[1]. These types of data integrity events, especially when they target an entire organization, can have a catastrophic impact on an enterprise and its ability to operate.

Typical attack vectors include ransomware, phishing, unmitigated vulnerabilities, and malicious/infected attachments. Once the malware gains a foothold in an organization, it can use multiple techniques to spread and corrupt data. The data at risk includes: active current data, backup data, system configurations, and baseline operating systems.

GOALS

This project will answer specific questions pertaining to data integrity and recovery such as:

- What data was corrupted? When was it corrupted? How was it corrupted? Who corrupted it?
- Do any other events coincide with this corruption?
- What was the impact of the data corruption?
- Which backup version should be used to recover data?

The data integrity solution derived from this project will include:

- a file system integrity solution to allow recovery from trusted backups and snapshots
- a database integrity approach with transactions and versioning to allow for rollbacks to a known good state
- an overall automated system that incorporates the previous two areas, as well as capabilities such as logging, restoration, and versioning

1 http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

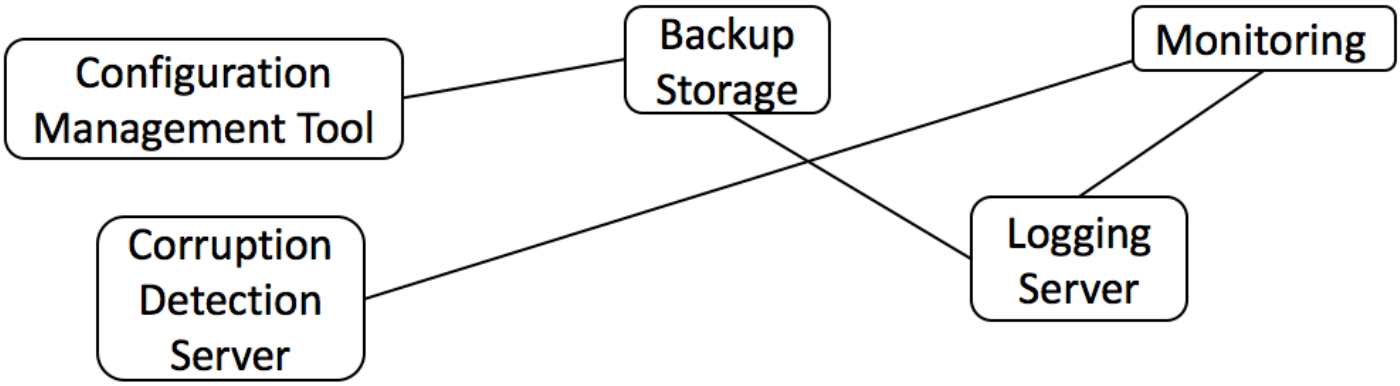
CONTACT US
di-nccoe@nist.gov
301-975-0200

BENEFITS

The potential business benefits of the data integrity solution explored by this project include:

- detecting backup data-tampering
- reducing the impact of a data-corruption event
- reducing downtime caused by data-corruption
- improving trustworthiness of backup data
- reducing the negative impact to the reputation of an organization due to data-corruption events
- providing management with improved continuity of operations

HIGH-LEVEL ARCHITECTURE



COMPONENTS

Our data integrity recovery solution includes, but is not limited to, the following components:

- file integrity monitors
- file versioning
- file integrity testing
- user activity monitoring
- configuration management
- database rollbacks
- virtual machine integrity/snapshots/versioning
- versioning file systems
- journaling file systems

DOWNLOAD THE PROJECT DESCRIPTION

For more information about this project, visit:
https://nccoe.nist.gov/projects/building_blocks/data_integrity

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interested in contributing technology or expertise to this project, please email di-nccoe@nist.gov.