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 NIST Cybersecurity Practice Guide SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*. 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.

CHALLENGE

Ransomware and other destructive events are decidedly on the rise. According to the FBI, ransomware payments are expected to cost companies $2 billion in 2017, compared with $1B spent in all of 2016[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.

1 https://www.cyberscoop.com/ransomware-2-billion-bitdefender-gpu-encryption/

SOLUTION

Data Integrity (DI) is meant to provide the capabilities to restore a system to its last known good state. The solution addresses a variety of operating systems and enterprise software. The example solution proposed here is designed to provide:

- secure storage capabilities for database backups
- automated logging, reporting, and alerting of DI events across the enterprise
- corruption testing capability that works in tandem with logging and alert functionality to recognize DI events
- backup capability that allows for the restoration of data to restore a system's last known good state
- virtual infrastructure support for the above

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

EXAMPLE SCENARIOS

Ransomware: Malware runs on a user's system and renders their data unusable unless a ransom is paid. The data integrity implementation identifies affected machines and facilitates restoration of the data.

System Manipulation by an Insider: Either through the execution of malware or through malicious intent, several compromised accounts are created on a system. The data integrity implementation notes the account creation and provides the means to restore the AD system to a safe state.

User Error: A user error causes the deletion of a critical Virtual Machine used by the company. The data integrity implementation helps to analyze the event and restore the virtual machine completely.

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

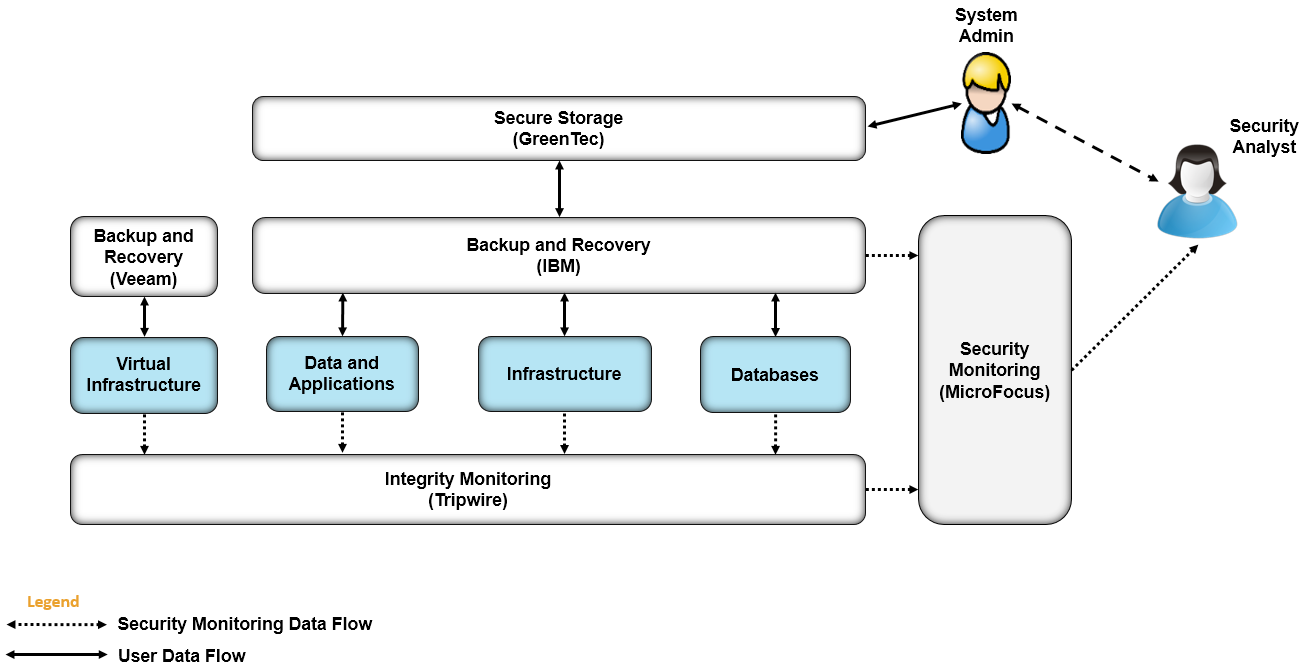
CONTACT US
di-nccoe@nist.gov
301-975-0200

Database Metadata: A poorly designed script causes a key database table to be moved to an unknown location. The data integrity implementation identifies the cause of the error and restores the database to a known good state.

Data Destruction: Malware runs on a user's system, modifying and deleting their data with no offer to recover it. The data integrity implementation identifies affected machines and facilitates the restoration of the data.

Transactional Database Changes: Database queries caused undesirable changes to a company's data. The data integrity implementation helps create a time line of events to determine the most effective means of restoration.

HIGH-LEVEL ARCHITECTURE



TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement to collaborate with NIST in a consortium to build this example solution.

GreenTec™ www.GreenTec-USA.com · IBM · MICRO FOCUS · tripwire · veeam

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit: https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/recover

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email di-nccoe@nist.gov.