Data Integrity: Recovering from Ransomware and Other Destructive Events

Tim McBride
NCCoE
NIST
Gaithersburg, MD
timothy.mcbride@nist.gov

Anne Palm Townsend
NCCoE
The MITRE Corporation
McLean, VA
apalm@mitre.org

Michael Ekstrom
NCCoE
The MITRE Corporation
Rockville, MD
mekstrom@mitre.org

Lauren Lusty
NCCoE
The MITRE Corporation
McLean, VA
lsharpe@mitre.org

Julian Sexton
NCCoE
The MITRE Corporation
Rockville, MD
jtsexton@mitre.org

***Abstract*—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 abstract provides an overview of the NIST Cybersecurity Practice Guide SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*.**

Key words—business continuity, data integrity, data recovery, malware, ransomware

I. Introduction

Data integrity (DI) attacks have compromised corporate information, including emails, employee records, financial records, and customer data. Destructive malware, ransomware, malicious insider activity, and even honest mistakes all set the stage for why organizations need to quickly recover from an event that alters or destroys data. Businesses must be confident that they can recover and that the recovered data is accurate and safe.

NCCoE at NIST built a laboratory environment to explore methods to effectively recover from a data corruption event in various IT enterprise environments.

II. Security Experiences

A. The Problem

When an organization's data sustains a DI attack, the attack can impact emails, employee records, financial records, and customer data, rendering the information unusable or unreliable or even cause operations to cease. When DI events occur, organizations must be able to recover quickly from the events and trust that the recovered data is accurate, complete, and free of malware.

B. The Solution

The NCCoE implemented a reference solution composed of secure storage, logging, virtual infrastructure, corruption testing, and backups that together enable recovery from a detected DI event. Secure storage is the ability to store files such as backups, gold images, or configuration files in a format that cannot be corrupted. The logging capability works in conjunction with corruption testing to detect changes in the integrity of information associated with monitored data, and generates logs about these events. These details can be used to investigate the logs to correlate all events relative to the attack across all items that report log files. A security analyst attempting to recover from a DI event would determine the "last known good" for the systems that the backup capability would employ for recovery. This backup capability would restore to the point prior to the DI event.

This reference solution creates the ability to understand the 'last known good' of an enterprise, to recover to that point, and resume operations quickly and efficiently.

III. Challenges and Obstacles

There is a trade-off between the frequency of backups and the amount of data loss an enterprise will experience. More frequent backups require more resources, both in work performed by the client and in space required on the server. More frequent backups, however, provide more granularity in recovery capabilities. Without proper balance, a file will lose more data during recovery because the restoration is to a point in time and will not reflect recent changes to the file.

Acknowledgment

We are grateful to the following individuals for their generous contributions of expertise and time: Steve Petruzzo (GreenTec USA), Steve Roberts (MicroFocus), Dave Larimer (IBM), John Unthank (IBM), Jim Wachhaus (Tripwire), Donna Koschalk (Veeam), Brian Abe (MITRE), Sarah Kinling (MITRE), Josh Klosterman (MITRE), Susan Urban (MITRE), Mary Yang (MITRE)

References

[1] T. McBride, et al., *Data Integrity: Recovering from Ransomware and Other Destructive Events*, NIST Special Publication 1800-11, National Institute of Standards and Technology, Gaithersburg, Md., September 2017. https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11b-draft.pdf

Identify applicable funding agency here. If none, delete this text box.