NIST SPECIAL PUBLICATION 1800-11A

Data Integrity

Recovering from Ransomware and Other Destructive Events

Volume A:
Executive Summary

Timothy McBride
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Michael Ekstrom
Lauren Lusty
Julian Sexton
Anne Townsend
The MITRE Corporation
McLean, VA

September 2020

FINAL

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-11

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/recover

Executive Summary

- Data integrity 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 recovered data is accurate and safe.
- The National Cybersecurity Center of Excellence (NCCoE) at NIST built a laboratory environment to explore methods to effectively recover from a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also explored auditing and reporting IT system use issues to support incident recovery and investigations.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions following a detected cybersecurity event. The solutions outlined in this guide encourage monitoring and detecting data corruption in commodity components—as well as custom applications and data composed of open-source and commercially available components.
- Thorough quantitative and qualitative data collection is important to organizations of all types and sizes. It can impact all aspects of a business including decision making, transactions, research, performance, and profitability, to name a few.

CHALLENGE

Organizations must be able to quickly recover from a data integrity attack and trust that any recovered data is accurate, complete, and free of malware. Data integrity attacks caused by unauthorized insertion, deletion, or modification of data have compromised corporate information including emails, employee records, financial records, and customer data. Some organizations have experienced systemic attacks that caused a temporary cessation of operations. One variant of a data integrity attack–ransomware–encrypts data and holds it hostage while the attacker demands payment for the decryption keys.

SOLUTION

The NCCoE developed and implemented a solution that incorporates appropriate actions in response to a detected cybersecurity event. If data integrity is jeopardized, multiple systems work in concert to recover from the event. The solution includes recommendations for commodity components and explores issues around auditing and reporting to support recovery and investigations.

While the NCCoE used a suite of commercial products to address this cybersecurity challenge, this guide does not endorse any particular products—nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts are responsible for identifying the available

products that will best integrate with your existing tools and IT system infrastructure. Your organization can choose to adopt this solution or one that adheres to these suggested guidelines or you can use this guide as a starting point for tailoring and implementing parts of the solution.

BENEFITS

This practice guide can help your organization:

- develop a strategy for recovering from a cybersecurity event
- facilitate a smoother recovery from an adverse event, maintain operations, and ensure the integrity and availability of data critical to supporting business operations and revenue-generating activities
- manage enterprise risk (consistent with foundations of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*)

SHARE YOUR FEEDBACK

You can view or download the Practice Guide at https://nccoe.nist.gov/projects/building_blocks/data_integrity.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging an in-person demonstration of this reference solution, email the project team at ds-nccoe@nist.gov.

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.

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.

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, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://nccoe.nist.gov
nccoe@nist.gov
301-975-0200