MANGAN INC. Cybersecurity

REAL Matters

Incident Recognition, Response and Reporting

ICSSbD Industrial Control Systems Secure by Design

Volume 1, Advisory #3 – April 2022

REAL Matters advisories are published to communicate cybersecurity threats and risks within the Operational Technology (OT) environment and where Critical Infrastructure vulnerabilities are identified. The purpose of this newsletter is to inform, propose suggested approaches to mitigate the risk as well as provide feedback on how Mangan Cybersecurity is approaching the issue(s) addressed.

Advisory Information

At A Glance

Issue Date:	April 19, 2022
Summary:	The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) codifies cybersecurity incident reporting to Cybersecurity and Infrastructure Security Agency (CISA)
Systems Impacted:	Critical infrastructure owners and operators.
Importance:	High

Details

Since the passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) the Cybersecurity and Infrastructure Security Agency (CISA) has been busy to define the rules the which will apply to the law. Requirements in the law apply to those critical infrastructure owners' and operators' responsibilities to report cybersecurity incidents as well as payments in response to ransomware attacks. The law also specifies processes for Federal agencies information reporting and sharing with CISA. While the law is aimed at the critical infrastructure, the premise of recognizing a cybersecurity incident event applies to any organization where both Information and Operations Technology architecture is vulnerable to attacks by threat actors. Mangan Cybersecurity's Industrial Control Systems Secure by Design (ICSSbD) Toolkit can measure the cybersecurity risk and specify controls and countermeasures for these threats.

The CIRCIA rulemaking process will determine what constitutes a reportable incident. Until then, CISA requests that critical infrastructure organizations continue to use the CISA reporting forms to share information pertaining to cybersecurity events. (refer to Sharing Cyber Event Information With CISA: Observe, Act, Report)

Actions and/or Recommendations

Mangan Cybersecurity ICSbD recognizes those activities specified by CISA and methods for recognizing the activity. DMZ firewalls and other OT logging capable equipment should undergo regular log and event reviews to determine any circumstance of unauthorized access. Alarm logs and operator maintenance requests where an OT device is down or inaccessible for more than 12 hours should be considered both in the context of maintenance for repair but also in the context of a Denial of Service (DOS) cybersecurity attack requiring scrutiny for the cause of failure. Regularly inspecting anti-virus, anti-malware scans, baseline record of Windows Registry settings, PLC hashes and other device configurations may identify malicious code drops. Examinations of failed log-in attempts should be followed-up for attempted threat actor activity. Inspecting the network communications for out-of-band activities as well as installing security appliances can identify malicious attempts to scan the OT network to understand the architecture and use.

About Mangan Inc.

Mangan Inc. is a nationally-recognized Specialty Engineering, Automation, and Integration company, providing a full-range of services to the Oil & Gas, Refining, Pipeline, Chemicals, and Life Sciences Industries. Established in Long Beach, California in 1990, Mangan's multiple office locations include sites in California, Georgia, New Hampshire, North Carolina, Texas, and Louisiana. Mangan's 350+ employee-owners bring expertise, innovation, and safety as their core mission to some of the largest companies in the world.