Press release

October 2, 2024
National Center of Incident Readiness and Strategy for Cybersecurity
National Police Agency

Co-sealing the Australian-Led International document on the Principles of Operational Technology Cyber Security

1. Overview

On October 2, 2024, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) co-sealed and published an international document entitled "Principles of operational technology cyber security" (hereinafter referred to as the "Document"). The Document was authored by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC). Tentative translations will be released as soon as possible.

The following nine countries co-sealed the Document and are listed in the Document: Australia, Japan, United States (US), United Kingdom (UK), Canada, New Zealand, Germany, Netherland and South Korea.

This Document is designed to assist critical infrastructure organisations relying on Operational Technology (OT) to provide their vital services. This Document describes six principles that assist organisations make decisions for designing, implementing, and managing OT environments. The NISC co-sealed the Document because the application of these principles to Japanese critical infrastructure organisations will contribute to strengthening cyber security in Japan.

The NISC will continue to make its efforts to foster international collaboration in the field of cybersecurity.

2. Overview of the Document

(1) Introduction

Critical infrastructure organisations rely on Operational Technology (OT) to control and manage the physical equipment and processes that provide vital services. The Document describes principles to assist organisations make decisions for designing, implementing, and managing OT environments in critical infrastructure organisations to ensure the safety and security of their OT environments as well as enable business continuity of vital services.

(2) Abstract of the six principles:

A) Principle 1: Safety is paramount

- ✓ Elements to consider: safety of human life, safety of plant, equipment and the environment, and the reliability and uptime of the critical infrastructure's services
- ✓ Questions to be asked at incident response: preparation to send appropriate staff to the site, trustworthiness of the backups, and so forth

B) Principle 2: Knowledge of the business is crucial

- ✓ Baseline:
  -Identify the vital systems the organisation needs to continue to provide their crucial services
  -Understand the OT system’s process, and the significance of each part of the process
- ✓ Integrate OT-specific incident response plans into the organisation’s other business continuity plans and to provide an information pack to third parties before or when they are engaged
- ✓ Understand the business context of the OT system for assessing the impact and criticality of OT outages and cyber security compromises.
- ✓ Maintain working relationships with OT cyber security personnel who have a working knowledge of plant operation in the organization responsible for the physical plant

C) Principle 3: OT data is extremely valuable and needs to be protected

- ✓ Protect engineering configuration data, such as network diagrams, and more ephemeral OT data, such as voltage or pressure levels, and so forth
- ✓ Seek to do more than protect the confidentiality, integrity and availability of OT data, such as alerting when OT data is exfiltrated

D) Principle 4: Segment and segregate OT from all other networks

- ✓ Segment and segregate their OT from all other networks
- ✓ Ensure adequate separation of the administration and management interfaces of OT system from their IT environment counterparts

E) Principle 5: The supply chain must be secure

- ✓ Re-evaluate the scope of systems that require oversight regardless of the size and engineering significance of vendors
- ✓ Consider what a device could do if its firmware or configuration was changed if the device is connected to a vendor, who can update the firmware.

F) Principle 6: People are essential for OT cyber security

- ✓ A mix of people with different backgrounds, with various skills, knowledge, experience and security cultures is necessary
- ✓ In most critical infrastructure OT sites, staff who are the front line of defense almost certainly will not be OT cyber security experts. As such, significant focus is required to develop cyber security awareness as a core component of field safety culture

(End)