NCCIC

National Cybersecurity and Communications Integration Center

Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Industrial Control Systems play an integral role in facilitating operations in each of the Nation's 16 critical infrastructure (CI) sectors, and they face increasing risk from cybersecurity threats. An organization's strategic cybersecurity goal is to protect the assets it deems critical to successful operation. Defense in Depth provides a flexible and usable framework for improving control system cybersecurity. Defense in Depth is based on a combination of people, technology, operations, and adversarial awareness. This fact sheet provides an outline of a holistic approach that an organization can use to improve its overall cybersecurity posture.

Basis for ICS Security Controls

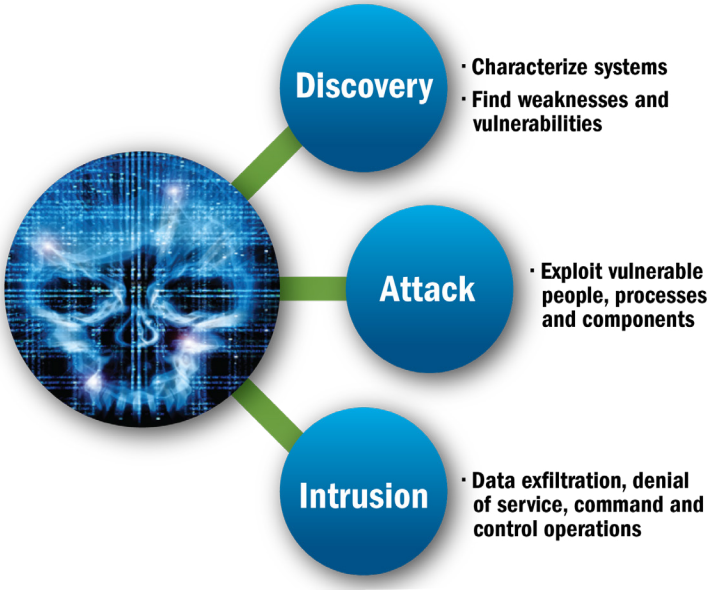
- Identification and Characterization of Risk
- Criticality-Based Asset Inventory
- Understanding Company Risk Appetite
- Implementation of Tailored Security Controls
- Using Communications Monitoring
- Physical Security Controls
- ICS Network Architecture
- Network Security Architecture

As technology evolves, it works its way into the ICS environment. This fact sheet highlights considerations associated with emerging technology.

Emerging Topics in ICS Security

- Bring Your Own Device (BYOD)
- Virtual Machine Technologies
- Security Monitoring in an ICS environment
- ICS Intrusion Detection and Prevention Systems
- Security Information and Event Management (SIEM) technologies
- ICS Supply Chain Management
- Managed Services and Outsourcing
- Leveraging Cloud Services in ICS

Understanding some of the more notable cyber attacks on ICS provides better understanding of how to apply security control improvements to your organization and ICS infrastructure. The cyber attack life-cycle includes three basic phases: discovery, attack, and intrusion.



Become familiar with different ICS attack methods and attack campaigns that use them:

ICS Attack Methods

- Exploiting Weak Authentication
- Network Scanning/Probing
- Removable Media
- Brute Force Intrusion
- Abuse of Access Authority
- Spear Phishing
- SQL Injection

Cyber attackers use attack methods to exploit cybersecurity weakness in people, technology, and processes. Attack campaigns discussed in the full document include Black Energy, Unauthorized Access Attacks, Database and SQL Data Injection Attacks, Dragonfly/Havex Attacks, and other scenarios.

The Defense-in-Depth Recommended Practice document provides the following recommendations for securing ICS:

- developing a proactive security model,
- leveraging sector and industry groups for standards and support, and
- accessing freely available tools and services from the DHS NCCIC program.

The full Defense-in-Depth Recommended Practice document is available on the https://ics-cert.us-cert.gov/.

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center