PROTECTING INDUSTRIAL CONTROL SYSTEMS

What You Need to Know

JUNE 2019
Protecting Critical Infrastructure

June 2019
Critical Infrastructure & Control Systems/Operational Technology

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments & Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation
- Water and Water Treatment

Many Still Running Windows XP
SYSTEM DIFFERENCES BY DESIGN & OPERATIONS

**IT systems emphasis: confidentiality**
- Enterprise information systems network
- ERP, CRM, email, financial systems
- Business-supporting applications
- Mature environment / routine patching & updates

**CS / Operational Technology emphasis: availability**
- Building management systems (BMS)
- Energy control (lights and efficiency)
- Environmental (heating, ventilation and air conditioning (HVAC))
- Security and safety (CCTV, access control, fire suppression)
- Ancillary systems (elevators, shade control, exterior lighting)
- PLC, SCADA, ICS, IIoT, HMI
- The “forgotten network” / rare patches & updates

*Many Irregularly Patched or Patch Doesn’t Make Secure; Undiscovered Adversary Presence > 200 days*
53% of OT/CS Networks at Risk Because of Legacy Windows Systems

• In critical infrastructure you should plan to be targeted. And if targeted, you will be compromised. It’s that simple.”

• 40% sites exposed to Internet via direct connection; an inevitable target for attackers and increasing overall attack surface of its associated critical infrastructure (air gap myth persists)

• 69% sites have plain text passwords traversing the network

• Legacy Windows installations no longer receive security updates from Microsoft and acting as open security gaps

Oct’18 2019 CYBERX
“Global ICS & IIoT Risk Report”
past 12 months 850+ production CS networks across 6 continents, all industrial sectors including energy and utilities, manufacturing, pharmaceuticals, chemicals, and oil and gas
• 2018 National Defense Strategy articulates DoD’s intent to invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations

• To enhance cybersecurity risk management for CS, DoD must implement standardized best practices, improve CS information sharing, advance cyber assessment capabilities, maintain CS training, and establish a reporting requirement to ensure CS cybersecurity accountability

• DoD Components will be accountable for:
  • Best Practices and Tactics, Techniques, and Procedures: Reduce operational risks posed by adversarial actions by implementing basic cybersecurity practices as well as proactively incorporating processes to harden CS infrastructure supporting Defense Critical Infrastructure (DCI)
  • Establishes firm dates to begin reporting completion

“CS consist of systems, devices, & networks designed to monitor or control specific processes (e.g. electricity & utility management, shipboard or aircraft mgt systems, building automation, fuel distribution management, & chemical measurements)”
RESPONSIBILITIES OF DOD COMPONENTS TO IMPLEMENT CYBERSECURITY FOR ALL DOD CONTROL SYSTEM (CS) TYPES

• Designate office of primary responsibility (OPR) to represent DoD Component on policy and procedural matters regarding cybersecurity for CS; Regardless of OPR designation, DoD Component CIOs are responsible for compliance with DoD cybersecurity standards in DoD IT / NSS, to include CS per Title 10 § 2223

• Ensure cybersecurity requirements for CS are addressed and visible to DoD Component CIOs in all portfolios, life-cycle management processes, and investment programs.

• Establish and/or employ blue & red team tools, capabilities, and test environments to proactively identify, reduce, & mitigate cybersecurity vulnerabilities & improve net defense

• Identify or establish and maintain cybersecurity education & training requirements for DoD personnel responsible for operating, maintaining, and monitoring CS & CS environments

“CS include Supervisory Control and Data Acquisition (SCADA), industrial and process controls systems, cyber-physical systems, facilities-related control systems and other types of industrial measurement and control systems”