Critical Infrastructure

Josh Wilcox (jw14g24)

May 9, 2025

Table of Contents

What are Critical Infrastructures

Definition of Critical Infrastructure

- Facilities, systems, sites, information, people, processes
- All **necessary for a country to function** and upon which **daily life depends**

Importance

- The loss or compromise of critical infrastructure would result in **major detrimental** impact on essential services
- Could lead to **significant loss of life** or have severe economic impacts

UK Critical Infrastructure Sectors

- **Essential Services:** Energy, Water, Food, Health, Emergency Services
- **Economic:** Finance, Transport, Communications
- **State Functions:** Government, Defence, Civil Nuclear
- **Advanced Infrastructure:** Chemical, Space, Digital Infrastructure

Industrial Control Systems (ICS)

Definition and Purpose

- Systems that monitor and control industrial processes
- Crucial for managing Critical Infrastructure operations
- Integrate hardware and software components

Key Components

- **SCADA (Supervisory Control and Data Acquisition)**
  - Centralized systems for monitoring and control
  - Collects real-time data from remote locations
- **Control Components**
  - RTUs (Remote Terminal Units) - Field data collection
  - MTUs (Master Terminal Units) - Central processing
  - PLCs (Programmable Logic Controllers) - Process automation
- **Interface Systems**
  - HMI (Human-Machine Interfaces) - Operator control panels
  - IEDs (Intelligent Electronic Devices) - Smart sensors/actuators

Applications

- Power generation and distribution
- Water treatment facilities
- Manufacturing processes
- Transportation systems

Cyber Security of CIs and ICSs

Legacy ICS components

- Old ICS components were not designed with security in mind
- They tended to use **security through obscurity**
  - Proprietary and unknown software, interfaces and protocols
  - Hackers that access the system can do a whole lot of damage

Stuxnet - Overview

Attack Infrastructure

- Targeted nuclear facility's Industrial Control System
- System was air-gapped (not connected to Internet)
- PLCs controlled physical equipment via assembly code
- Infection likely through USB devices and LAN spread

Key Lessons

- Demonstrated sophisticated cyber-physical attack methodology
- Used legitimate ICS features rather than zero-days
- Showed vulnerability through supply chain weak links
- Proved indirect infiltration possible via soft targets

Stuxnet - Strategic Implications

Advantages Over Traditional Attacks

- Avoided casualties and physical destruction
- Prevented severe retaliation
- Minimized collateral damage (e.g., oil prices)

Cyber Weapon Challenges

- Can be copied and reused
- Proliferation cannot be controlled
- Near-impossible attack attribution
- Plausible deniability for attackers
- Traditional deterrence ineffective

BlackEnergy - Ukraine Power Grid Attack

Attack Overview (December 2015)

- Affected three energy distribution companies
- 225,000 customers lost power (1-6 hours)
- Disabled IT infrastructure
- Removed critical files
- DoS attack on call center

Attack Method

- Started with spear-phishing campaign
- Gained network access via malicious macros
- Mapped network through VPN credentials
- Accessed SCADA through HMI hijacking
- Disabled systems with KillDisk and MBR wiping

BlackEnergy - Key Lessons

Security Recommendations

- Implement phishing awareness training
- Use endpoint protection and application whitelisting
- Monitor network traffic anomalies
- Properly segregate IT and SCADA networks
- Implement strong VPN security
  - Two-factor authentication
  - Session timeouts
- Apply separation of duties in SCADA systems
- Avoid default/shared credentials

Summary

Key Points

- Critical Infrastructure (CI)
  - Essential facilities, systems, and processes
  - Vital for country's function and daily life
- Industrial Control Systems (ICS)
  - Control and monitor CIs
  - Complex integration of hardware and software
- Case Study Lessons
  - Stuxnet: Sophisticated cyber-physical attacks possible
  - BlackEnergy: Importance of comprehensive security