SECURITY CONSIDERATIONS FOR CRITICAL INFRASTRUCTURE

CANADIAN CENTRE FOR CYBER SECURITY

APRIL 2022 | ITSAP.10.100

Critical infrastructure (CI) plays a role in the delivery and support of the necessities of daily life. This includes commonly used services, such as water, hydro, and finances. Disruptions to CI could result in loss of vital services, harm to the public, or even loss of life. This document provides information on how CI sectors can be compromised and what security measures can be implemented to mitigate the risks.

WHAT IS CI?

CI refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CIs are often interconnected and interdependent within and across provinces, territories, and national borders. The *National Strategy for Critical Infrastructure* identifies the following ten CI sectors:

Energy and Utilities

Finance

Food

Government

Health

Information and communication technology

Manufacturing

Safety

Transportation

Water

OPERATIONAL TECHNOLOGY (OT) AND INDUSTRIAL CONTROL SYSTEMS (ICS) AS THREAT TARGETS

OT includes computing systems used to automate industrial processes and operations in many different sectors, such as manufacturing. ICS is a major subset within OT that allows CI providers to remotely monitor their processes and control their physical devices on their infrastructure.

OT and ICS that are connected to the Internet or to other networks and systems are attractive targets to threat actors, who may be focused on disruption of OT or ICS, or compromising them as pathways for phishing schemes, spam, or malware attacks.

MAIN THREATS TO CI

Cybercrime threat actors may target CI sectors for financial gains. Some CI sectors, such as health care and manufacturing, are popular targets because their owners and operators cannot tolerate long-term disruption of essential services and often have significant financial resources to pay ransom. Insider threat actors may target for personal reasons, such as an act of revenge by disgruntled former employees or customers. State-sponsored cyber threat actors may target CI sectors to collect information in support of broader strategic goals to influence public opinion or development of policy.

Cyber threats to CI sectors can involve stealing mission-critical information, locking sensitive files, or leaking proprietary or compromising information. Some of the main cyber threats to CI include:

Ransomware is a form of malware that denies users access to systems or data until a sum of money is paid. Other types of malware (e.g. wipers and spyware) are used to target CI by infiltrating or damaging connected systems.

Denial-of-service (DoS) is any activity that makes a service unavailable for use by legitimate users, or that delays system operations and functions. A threat actor could render large parts of a CI sector unavailable and cause potentially catastrophic failure.

Insider threats can result from anyone who has knowledge of or access to an organization's infrastructure and information and uses it, either knowingly or inadvertently, to cause harm. Insider threats could have a significant impact on a CI sector and its business functions.

Damage to CI can threaten national security, public safety, and economic stability

Communications Security Establishment | Centre de la sécurité des télécommunications

© Government of Canada | This document is the property of the Government of Canada. It shall not be altered, altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE. Cat. No. D97-1/10-100-2022E-PDF ISBN 978-0-660-42803-1

Canada

SECURITY CONSIDERATIONS FOR CRITICAL INFRASTRUCTURE

CANADIAN CENTRE FOR CYBER SECURITY

APRIL 2022 | ITSAP.10.100

WHAT ARE THE IMPACTS?

Cyber attacks on CIs can have serious and devastating consequences. Here are just some of the potential ones:

- interruption of basic essential services we all rely on such as electricity, water and natural gas
- disruption in production and supply of food and medical supplies
- loss of overall public trust and confidence in the economy, national security and defence as well as in the democratic processes
- damage to the environment and risk to public health from chemical spills, toxic waste discharges or hazardous air emissions
- lost revenue, reputational risks, job losses, or legal consequences (e.g. liability from a data breach) for companies and employees
- disruptions to hospital operations, or even compromised medical devices, that could lead to loss of life

LEARN MORE

Visit our website at **cyber.gc.ca** to find a catalogue of cyber security publications, including:

- Security considerations for industrial control systems (ITSAP.00.050)
- Protect Your Organization from Malware (ITSAP.00.057)
- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)
- Virtualizing your Infrastructure (ITSAP.70.011)
- Protective Domain Name System (ITSAP.40.019)
- Ransomware Playbook (ITSM.00.099)
- Don't Take the Bait: Recognize and Avoid Phishing Attacks (ITSAP.00.101)
- Tips for Backing up Your Information (ITSAP.40.002)
- Ransomware: How to Prevent and Recover (ITSAP.00.099)
- Secure your accounts and devices with multi-factor authentication (ITSAP 30.030)
- Offer Tailored Cyber Security Training to Your Employees (ITSAP.10.093)
- Protect Your Organization from Insider Threats (ITSAP.10.003)

HOW TO PROTECT YOUR CI SECTOR FROM CYBER ATTACKS

CI network operators can reduce their risks of cyber attack by implementing the following security measures. For more info on mitigation measures check out the CISA advisory (link available in English only).

Isolate CI components and services by implementing firewalls, virtual private networks (VPN), and multi-factor authentication (MFA) for remote access connections with corporate networks. When using ICS, test manual controls to ensure critical functions remain operable if your network is unavailable or untrusted. Use Privileged Access Workstations (PAWs) to separate sensitive tasks and accounts from non-administrative computer uses, such as email and web browsing. Implement network security zones to control and restrict access and data communication flows to certain components and users. *Be prepared under imminent threat to isolate CI components and services from the internet.*

Enhance your security posture by automatically patching your operating systems and applications. Replace devices and products that are past their end of life. Implement offline backups that are tested frequently to ensure you can recover quickly in the event of an incident.

Protect your network from malware by virtualizing your network to prevent it from spreading and infecting your corporate networks. Deploy network and endpoint monitoring through securely configured and enabled anti-virus and anti-malware software, and activate software firewalls on connected devices.

Develop an incident response plan that includes the processes, procedures, and documentation related to how your organization detects, responds to, and recovers from cyber attacks. Test and revise the plan periodically to ensure critical functions and operations continue in case of system disruptions or unexpected downtime.

Train your employees so they understand the importance of cyber security best practices, such as identifying malicious emails and links, using passphrases or strong passwords, and reporting incidents as soon as they are detected.

Monitor organizational activities by collecting, analyzing, and storing records that are associated with user actions on information systems. Enable logging in order to better investigate issues or events. Monitor traffic at your Internet gateways and establish baseline of normal traffic patterns. Highly sophisticated threat actors may influence or coerce employees (e.g., social engineering, bribery, blackmail, intimidation) to help them compromise security. To guard against these actors, enhance your insider threat monitoring and consider implementing a "two-person" rule when performing critical administrative functions.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

© Government of Canada | This document is the property of the Government of Canada. It shall not be altered, altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE. Cat. No. D97-1/10-100-2022E-PDF ISBN 978-0-660-42803-1