TLP: WHITE

Transportation Security Administration

Pipeline Cyber Risk MITIGATION

The Cybersecurity and Infrastructure Security Agency (CISA) and the **Transportation Security Administration (TSA)** developed this infographic to outline activities that pipeline operators can undertake to improve the cybersecurity of their information technology (IT) and operational technology (OT) systems, and mitigate their exposure to some common risks.

Overview: The integration of information communication technologies (ICT), such as remote access and internet-connected devices, into pipeline networks improves operational efficiency and safety for pipeline owners and operators. However, integrating ICT into pipeline industrial control systems (ICS) may increase the attack surface nefarious cyber actors can exploit and, as a result, increases the amount of security required to both protect the devices and monitor their network activity.

Boundary Protection

Boundary protection involves establishing secure sub-networks for critical and operational ICS functions to prevent unauthorized access and communication. Without segmentation, an adversary may have easier and direct access to an ICS environment from the corporate network or through internet-connected devices located in the ICS environment.

MITIGATION

- Block direct access to and from the ICS to the internet unless secured through a proxy on the corporate network or VPN, with encryption and multi-factor authentication.
- Separate OT/ICS environment from corporate network(s) with multiple layers of firewalls and segments.
- Block traffic not expressly permitted by firewall policy (i.e., deny by default).
- Restrict communications to the ICS environment to essential business functions.
- Use different end user devices, such as dedicated and hardened laptops, to access/administer the internet technology (IT) and operational technology (OT) environments.

HISTORICAL EXAMPLE: In 2017, an actor installed malware on safety instrumented systems (SIS) at a petrochemical facility in Saudi Arabia in an attempt to cause damage and injuries. A lack of isolation of the critical SIS from the ICS network likely contributed to the compromise.

Monitoring

Monitoring entails the implementation of technologies and procedures to capture, monitor, and review network and host traffic in both IT and OT networks and establish a baseline of expected behavior in order to detect suspicious activity. Without effective monitoring capabilities in an ICS environment, operators may not be able to identify abnormal traffic.

MITIGATION

- Conduct network baseline analysis on ICS systems and networks to understand approved communication flows.
- Investigate and validate every communication to a new IP address or domain from the OT environment.
- Understand and disable unnecessary services and ports on OT systems; perform deep packet inspections or conduct manual network dataflow analysis.
- Monitor for abnormal traffic and user behavior such as simultaneous logins, VPN and/or TOR traffic, outside the office logins, or logins occurring outside normal business hours.

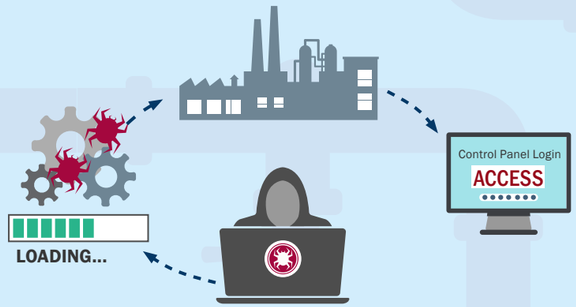
HISTORICAL EXAMPLE: In 2014, an actor deployed malware against Energy sector companies that provided espionage and persistent access, with sabotage as an optional capability. Monitoring unauthorized HTTP traffic coming out of the ICS network would likely have defended against this malware.

Configuration Management

Configuration management is a collection of activities focused on establishing and maintaining the integrity of products and systems, through controlling of the processes for initializing, changing, and monitoring the configurations of those products and systems. A poor configuration management program may result in operators not being able to distinguish between legitimate and, malicious or nefarious activity.

MITIGATION

- Maintain a baseline of expected programming language and configurations for OT devices.
- Periodically verify the logic and configuration of OT devices is correct; observe network traffic to identify attempts to change OT device configurations; observe network traffic to extract ladder logic files traversing the wire.
- Audit and actively monitor software, firmware, versions, patches, etc., noting the date installed and by whom for all devices.
- When possible, validate the authenticity of downloads (e.g., patches, updates) using cryptographic methods; never load updates from unverified sources.
- Enforce policy prohibiting any change without following the documented change approval processes.



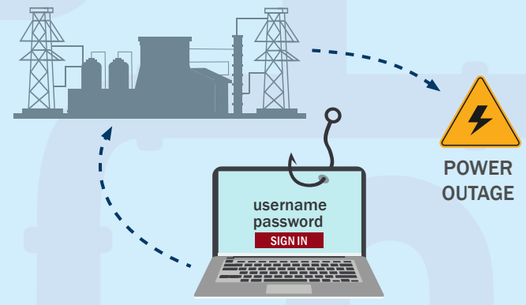
HISTORICAL EXAMPLE: In 2014, a cyber actor compromised 3rd party vendor websites, resulting in ICS operators downloading seemingly legitimate software, some of which was used for VPN access to PLC devices.

Access Control

Access control is the process of granting IT or OT system resources only to authorized users, programs, processes, or other systems. Poor access control can expose the organization to unauthorized access of data and programs, fraud, or the shutdown of computer services.

MITIGATION

- Restrict access to the OT environment to necessary personnel; audit accounts to ensure credentials are maintained, updated, and eliminated.
- Where possible, enable strong passwords, use multi-factor authentication, and account lockout policies to defend against attacks.
- Restrict users' permissions to install and run unauthorized software applications.
- Leverage encryption such as VPN when using untrusted networks or require remote access.
- Have mutually exclusive user account and password policies between IT and OT and do not use the same trust store in both environments.
- Change default vendor passwords on devices, applications and systems.



HISTORICAL EXAMPLE: In 2016, an actor used a phishing campaign to steal credentials and gain access to the ICS environment of a Ukrainian electric utility. The actor subsequently shut down a transmission substation causing blackouts in Kiev.

[1]The risks outlined above, while not comprehensive, represent commonly understood challenges across sectors that rely on ICT integration with OT systems.
[2]The mitigation methods provided above are not all-encompassing, but are examples of mitigation methods that could lower an entity's level of risk. For more information regarding mitigation methods, or to report suspicious activity, please reach out to **Central@cisa.gov**.