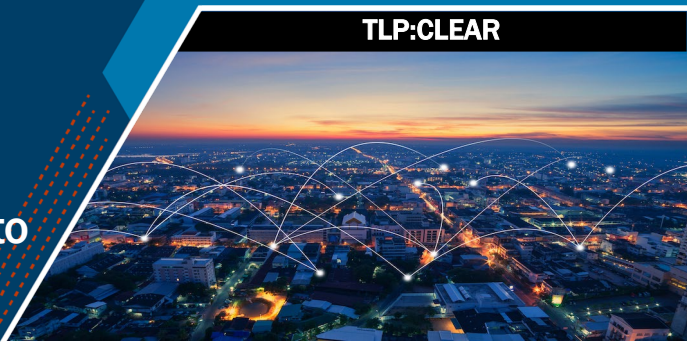

Primary Mitigations to Reduce Cyber Threats to Operational Technology

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Environmental Protection Agency (EPA), and Department of Energy (DOE)—hereafter referred to as "the authoring organizations"—are aware of cyber incidents affecting the operational technology (OT) and industrial control systems (ICS) of critical infrastructure entities in the United States. The authoring organizations urge critical infrastructure entities to review and act now to improve their cybersecurity posture against cyber threat activities specifically and intentionally targeting internet connected OT and ICS.

Mitigations

The authoring organizations recommend critical infrastructure asset owners and operators implement the following mitigations[1] to defend against OT cyber threats.

- **Remove OT connections to the public internet.** OT devices are easy targets when connected to the internet. OT devices lack authentication and authorization methods that are resistant to modern threats and are quickly found by searching for open ports on public IP ranges with search engine tools to target victims with OT components [CPG 2.X].
  - Cyber threat actors use simple, repeatable, and scalable toolsets available to anyone with an internet browser. Critical infrastructure entities should identify their public-facing assets and remove unintentional exposure.
- **Change default passwords immediately and use strong, unique passwords.** Recent analysis of this cyber activity indicates that targeted systems use default or easily guessable (using open source tools) passwords. Changing default passwords is especially important for public-facing internet devices that have the capability to control OT systems or processes [CPG 2.A][CPG 2.B][CPG 2.C].

[1] These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

- **Secure remote access to OT networks.** Many critical infrastructure entities, or contractors working on their behalf, make risk-based tradeoffs when implementing remote access to OT assets. These tradeoffs deserve careful reevaluation. If remote access is essential, upgrade to a private IP network connection to remove these OT assets from the public internet and use virtual private network (VPN) functionality with a strong password and phishing-resistant multifactor authentication (MFA) for user remote access.
  - **Document and configure** remote access solutions to apply principles of least privilege for the specific asset and user role or scope of work [CPG 2.H]. Further, disable dormant accounts.
- **Segment IT and OT networks**. Segmenting critical systems and introducing a demilitarized zone for passing control data to enterprise logistics reduces the potential impact of cyber threats and reduces the risk of disruptions to essential OT operations [CPG 2.F].
- **Practice and maintain the ability to operate OT systems manually.** The capability for organizations to revert to manual controls to quickly restore operations is vital in the immediate aftermath of an incident. Business continuity and disaster recovery plans, fail-safe mechanisms, islanding capabilities, software backups, and standby systems should all be routinely tested to ensure safe manual operations in the event of an incident.

The authoring organizations recommend that critical infrastructure organizations regularly communicate with their third-party managed service providers, system integrators, and system manufacturers who may be able to provide system-specific configuration guidance as they work to secure their OT.

- Misconfigurations may be introduced during standard operations, by the system integrator, by a managed service provider, or as part of the default product configuration by the system manufacturer. Working with the relevant groups to address these issues may prevent future unintentional vulnerabilities from being introduced.

Resources

CISA recommends critical infrastructure organizations review and implement, if possible, the following resources to enhance their security posture.

1. For an overview of tools to help identify public-facing devices on the internet and ways to reduce your internet attack surface, see CISA's Stuff off Search web page.
2. For more information on using strong passwords, see CISA's Use Strong Passwords web page.
3. For more information on phishing-resistant MFA, see CISA's Implementing Phishing-Resistant MFA fact sheet.
4. For more information on network segmentation, see CISA's Layering Network Security Through Segmentation fact sheet.
5. For more information on procuring Secure by Design OT components, see CISA's Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products.
6. For more information on top cyber actions to secure water systems and accompanying resources, see Top Cyber Actions for Securing Water Systems.

7. For more information on addressing network segmentation for water systems, please see EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems, Factsheet 2.F.
8. For more comprehensive security controls to address advanced threat actors who pivot through enterprise networks to reach OT, see Identifying and Mitigating Living Off the Land Techniques.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by the authoring organizations.

Please share your thoughts with us via our anonymous product survey; we'd welcome your feedback.