CISA INSIGHTS

PREPARING FOR AND MITIGATING POTENTIAL CYBER THREATS

December 15, 2021

Summary

In the lead up to the holidays and in light of persistent and ongoing cyber threats, CISA urges critical infrastructure owners and operators to take immediate steps to strengthen their computer network defenses against potential malicious cyber attacks. Sophisticated threat actors, including nation-states and their proxies, have demonstrated capabilities to compromise networks and develop long-term persistence mechanisms. These actors have also demonstrated capability to leverage this access for targeted operations against critical infrastructure with potential to disrupt National Critical Functions.

Executives and senior leaders can proactively take steps to prepare their organizations should an incident occur. Implementing the cybersecurity best practices provided below can help guide leaders to strengthen operational resiliency by improving network defenses and rapid response capabilities.

Actions for Leaders

CISA strongly urges organizations to take the following immediate actions to strengthen their defenses.

1. **Increase organizational vigilance** by ensuring there are no gaps in Information Technology (IT)/Operational Technology (OT) security personnel coverage and that staff provides continual monitoring for all types of anomalous behavior. Security coverage is particularly important during the winter holiday season when organizations typically have lower staffing.
2. **Prepare your organization for rapid response** by adopting a state of heightened awareness. Create, update, or review your cyber incident response procedures and ensure your personnel are familiar with the key steps they need to take during and following an incident. Have staff check reporting processes and exercise continuity of operations plans to test your ability to operate key functions in an IT-constrained or otherwise degraded environment. Consider your organization's cross-sector dependencies and the impact that a potential incident at your organization may have on other sectors, as well as how an incident at those sectors could affect your organization.
3. **Ensure your network defenders implement cybersecurity best practices.** Enforce multi-factor authentication and strong passwords, install software updates (prioritizing known exploited vulnerabilities), and secure accounts and credentials.
4. **Stay informed about current cybersecurity threats and malicious techniques.** Encourage your IT/OT security staff to subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.
5. **Lower the threshold for threat and information sharing.** Immediately report cybersecurity incidents and anomalous activity to CISA and/or the FBI.

Critical Infrastructure Resilience

Organizations with OT/Industrial Control Systems (ICS) assets can also improve their cyber posture and functional resilience by:

- **Identifying and securing critical processes** that must continue uninterrupted in order to provide essential services;
- **Developing and regularly testing workarounds or manual controls** to ensure that critical processes—and the ICS networks supporting them—can be isolated and continue operating without access to IT networks, if needed; and
- **Ensuring backup procedures are implemented and regularly tested,** and that backups are isolated from network connections.

Incident Response

If your organization is impacted by an incident or suspected incident:

- Implement your cyber incident response plan. See CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks for incident response practices and operational procedures and follow guidance in the joint cybersecurity advisory by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom on Technical Approaches to Uncovering and Remediating Malicious Activity for incident response best practices.
- Report incidents or anomalous activity immediately to CISA (mailto:central@cisa.govor 888-282-0870).
- Consider soliciting support from a third-party IT organization to provide subject matter expertise.

Resources

- Refer to CISA's Cyber Essentials for additional recommendations on managing cybersecurity risks.
- See Questions Every CEO Should Ask About Cyber Risks for additional best practices to help companies understand their risks and prepare for cyber threats.
- See CISA's Recommended Cybersecurity Best Practices for Industrial Control Systems for more guidance specific to organizations supporting U.S. critical infrastructure.
- See CISA's Cyber Resilience Review webpage for more information on CISA's no-cost, non-technical assessment to help organizations evaluate their operational resilience and cybersecurity practices.
- See CISA's Fact Sheet Rising Ransomware Threats to Operational Technology Assets for more information on reducing the vulnerability to ransomware or risk of severe business degradation if affected by ransomware. Although tailored to ransomware, the Fact Sheet has applicable guidance for other cyber threats.