January 18, 2022

Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats

Every organization in the United States is at risk from cyber threats that can disrupt essential services and potentially result in impacts to public safety. Over the past year, cyber incidents have impacted many companies, non-profits, and other organizations, large and small, across multiple sectors of the economy.

Most recently, public and private entities in Ukraine have suffered a series of malicious cyber incidents, including website defacement and private sector reports of potentially destructive malware on their systems that could result in severe harm to critical functions. The identification of destructive malware is particularly alarming given that similar malware has been deployed in the past—e.g., NotPetya and WannaCry ransomware—to cause significant, widespread damage to critical infrastructure.

This CISA Insights is intended to ensure that senior leaders at every organization in the United States are aware of critical cyber risks and take urgent, near-term steps to reduce the likelihood and impact of a potentially damaging compromise. All organizations, regardless of sector or size, should immediately implement the steps outlined below.

Reduce the likelihood of a damaging cyber intrusion

- ☐ Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
- ☐ Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.
- ☐ Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- ☐ If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.
- ☐ Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

Take steps to quickly detect a potential intrusion

- ☐ Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- ☐ Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- ☐ If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Ensure that the organization is prepared to respond if an intrusion occurs

- ☐ Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/ responsibilities within the organization, including technology, communications, legal and business continuity.
- ☐ Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- ☐ Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the organization's resilience to a destructive cyber incident

- ☐ Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.
- ☐ If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

By implementing the steps above, all organizations can make near-term progress toward improving cybersecurity and resilience. In addition, while recent cyber incidents have not been attributed to specific actors, CISA urges cybersecurity/IT personnel at every organization to review Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. CISA also recommends organizations visit StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.

As the nation's cyber defense agency, CISA is available to help organizations improve cybersecurity and resilience, including through cybersecurity experts assigned across the country. In the event of a cyber incident, CISA is able to offer assistance to victim organizations and use information from incident reports to protect other possible victims. All organizations should report incidents and anomalous activity to CISA and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.