Akin®

CISA Recommends Cybersecurity "Best Practices" in Advance of Winter Holidays

Dec 16, 2021

Reading Time : **1 min**

By: Scott Daniel Johnson

CISA warned that "[s]ophisticated threat actors, including nation-states and their proxies, have demonstrated capabilities to compromise networks and develop long-term persistence mechanisms," as well as "capability to leverage this access for targeted operations against critical infrastructure with potential to disrupt National Critical Functions," which are "functions of government and private industry so vital that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, and public health or safety," including, for example, the generation, transmission and distribution of electricity. (See here).

CISA provided a number of proactive "best practices" that entities can take to "strengthen operational resiliency by improving network defenses and rapid response capabilities." Its principal recommendations are to:

1. "Increase organizational vigilance by ensuring there are no gaps in Information Technology (IT)/Operational Technology (OT) security personnel coverage [during the holiday season, when staffing may be reduced,] and that staff provides continual monitoring for all types of anomalous behavior."
2. "Prepare your organization for rapid response by adopting a state of heightened awareness." This includes creating, updating or reviewing, as applicable, cybersecurity incident response procedures and continuity plans, and ensuring that personnel know what to do during and after an incident, so they can continue to "operate key functions in an IT-constrained or otherwise degraded environment."
3. "Ensure your network defenders implement cybersecurity best practices" such as using multifactor authentication and strong passwords for access to systems, installing

approved software updates (while "prioritizing known exploited vulnerabilities") and securing accounts and access credentials.

4. "Stay informed about current cybersecurity threats and malicious techniques," including by keeping up with CISA notifications about security topics and known threats.

5. "Lower the threshold for threat and information sharing" and "[i]mmediately report cybersecurity incidents and anomalous activity to CISA and/or the FBI."

CISA also provided additional actions to improve general cybersecurity hygiene, enhance functional resilience and speed incident response capabilities, as well as links to resources for additional information and guidance. Best wishes for safe and healthy winter holidays for all.

Categories

Oil & Gas | Transmission | Smart Grid/Energy Storage | Lobbying & Public Policy | Power | Renewable Energy | North America