American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

July 21, 2024

Microsoft Develops New Recovery Tool to Assist with CrowdStrike Issue Impacting Windows Endpoints

CrowdStrike says outage is NOT a security incident or cyberattack

A non-malicious global technology outage that began early Friday morning is continuing to affect many industries and is having varying effects on hospitals and health systems across the country.

The AHA remains in close communication with both Microsoft and CrowdStrike leadership to urgently relay clinical and operational disruptions occurring in hospitals across the country as a result of Microsoft computer outages caused by the faulty CrowdStrike update.

Yesterday evening Microsoft published a recovery tool to aid in the recovery of systems.

AHA National Advisor for Cybersecurity and Risk John Riggi said, “Recovery of hospital computer systems impacted by this outage is in full progress. For those hospitals that remain impacted, The Microsoft recovery solution may be able to accelerate recovery. We appreciate the responsiveness of both Microsoft and CrowdStrike and we will continue to engage their leadership to directly relay the operational, financial and clinical impact America’s hospitals and health systems are experiencing due to the CrowdStrike update.

CrowdStrike’s webpage includes more information about the issue. In addition, view the Cybersecurity and Infrastructure Security Agency alert on the incident. As a reminder, the following actions were highlighted in a July 19 Cybersecurity Advisory that hospitals and health systems could take.

WHAT YOU CAN DO:

- Share this Advisory with your IT and cybersecurity teams.
- If you have instances of CrowdStrike in your networks, determine the impact and review your business and clinical continuity procedures.
- Use this opportunity to identify impact and downtime procedures for all internal and third-party life-critical and mission-critical technology, services and supply chain.
- Test cyber incident response and emergency preparedness plans and communication channels.

- Plan for technology disruptions and cyber incidents on a regional basis.
- Be alert to increased phishing emails that may appear related to this disruption.
- Report any clinical impacts that your organization is experiencing to state and local public health officials as appropriate or required. You also may share information with the AHA by emailing Riggi at jriggi@aha.org.

FURTHER QUESTIONS

If you have further questions, please contact Riggi at jriggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.