American Hospital Association™
Advancing Health in America

Special Bulletin

October 29, 2020

New Information on Imminent Ransomware Threat against U.S. Hospitals

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) last night issued a joint advisory warning of credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers.

The agencies are urging the heath care sector to maintain business continuity plans — the practice of executing essential functions through emergencies (e.g. cyberattacks) — to minimize service interruptions, and follow federal best practices in the areas of network security, ransomware and user awareness.

Additionally, system administrators are urged to immediately take steps to ensure current, air-gapped backups are in place for all sensitive or proprietary data, especially if there is any indication of a network compromise. According to the Department of Homeland Security, hospitals and health systems are advised to develop emergency contingency plans should the attackers target multiple hospitals simultaneously in the same region.

The government has advised that phishing emails are the primary methodology to deliver the malware into victim organizations, but not the exclusive methodology. Therefore, email security should be increased and staff should be placed on heightened alert for suspicious emails.

"The AHA is working closely with government agencies to better understand the nature of the threat and assist in the exchange of threat information with hospitals across the nation," said John Riggi, AHA Senior Advisor for Cybersecurity and Risk. "The threat as we know it involves Trickbot malware and Ryuk ransomware targeting hospitals and health systems. Health care providers should proactively implement certain cybersecurity measures such as ensuring current, air-gapped backups of electronic health records and clinical and non-clinical data, expediting patching of all internet facing resources and test incident response plans as soon as possible. Hospitals should also be prepared to re-route patients to hospitals outside their area if there is a simultaneous regional outage of multiple-hospital IT systems. We will continue to monitor and work closely with our federal partners and distribute new details with members as they emerge."

FURTHER QUESTIONS

If you have questions, please contact John Riggi, at jriggi@aha.org.