American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

March 21, 2022

President Urges Immediate Hardening of U.S. Cyber Defenses Due to Potential Russian Strike

President Biden today urged an immediate hardening of private-sector cyber defenses "based on evolving intelligence that the Russian Government is exploring options for potential cyberattacks."

In tandem with the President's statement, the White House issued a fact sheet detailing steps organizations can take to protect against potential cyberattacks. Foremost among those steps are the implementation and mandated use of multi-factor authentication.

The AHA is closely monitoring the potential for increased cyber risks to the U.S. health system stemming from the ongoing military operations in the Russia/Ukraine region.

The Russian military has previously used cyberattacks against Ukraine to disrupt the electrical grid, communications capabilities and financial institutions. For example, destructive malware variants were found on Ukrainian networks in the period prior to Russia's invasion and it was reported recently that cyber denial-of-service attacks, attributed to the Russian military, were launched against Ukraine's Ministry of Defense, as well as its financial institutions and communications services. In 2017, the Russian military intelligence service launched the destructive NotPetya malware against Ukraine, which inflicted significant collateral damage to the U.S. health care sector.

As part of AHA's efforts, John Riggi, the association's national advisor for cybersecurity and risk, and a former senior executive in the FBI's cyber division, remains in close coordination with the FBI, Cybersecurity and Infrastructure Security Agency and the Department of Health and Human Services regarding related threats which may pose a risk to U.S. health care.

WHAT YOU CAN DO

- Share this Cybersecurity Advisory with your organization's IT and cyber infrastructure teams.

- Hospitals and health systems should visit AHA.org to review alerts and bulletins for guidance on risk mitigation procedures, including increased network

monitoring for unusual network traffic or activity, especially around active directory. Additionally, it is important to heighten staffs' awareness of increased risk of receiving malware-laden phishing emails.

- Geo-fencing for all inbound and outbound traffic originating from, and related to, Russia, Ukraine and its surrounding region may help mitigate direct cyber risks presented by this threat; however, it will have limited impact in reducing indirect risk, in which malware transits through other nations, proxies and third parties.

- AHA also recommends that organizations identify all internal and third-party mission-critical clinical and operational services and technology; in doing so they should put into place four-to-six week business continuity plans and well-practiced downtime procedures in the event those services or technologies are disrupted by a cyberattack.

- It is essential at this time to check the redundancy, resiliency and security of your organization's network and data backups, and ensure that multiple copies exist: off-line, network segmented, on premises and in the cloud, with at least one immutable copy.

- Ensure that emergency electric generating redundancy, resiliency and generator fuel reserves are in place and have been recently tested.

- It is also critical that a cross-function, leadership-level cyber incident response plan be fully documented, updated and practiced. This should include emergency communications plans and systems.

FURTHER QUESTIONS

If you have any questions or information regarding these issues, contact John Riggi at jriggi@aha.org.