American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

Feb. 23, 2022

U.S. Declares Start of Russia's Invasion of Ukraine, Introduces Sanctions; "Cyber Shields Up," Says CISA

President Biden on Feb. 22 announced that Russia's invasion of Ukraine has begun, with Russian military assets crossing into Ukraine's eastern provinces under the guise of a "peacekeeping" mission. The U.S. government and NATO allies immediately responded to Russia's actions with a series of economic and military sanctions. Now there is a concern that Russia may retaliate against the U.S. and allied nations with disruptive cyberattacks in furtherance of its military and political objectives.

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, it was reported last week 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.

In light of previous attacks and potential threats, the Cybersecurity and Infrastructure Security Agency last week issued a related-and-rare cyber "Shields Up" warning to the U.S. private sector, including health care, based upon the increased cyberthreat posed by the Russian government.

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, CISA and the Department of Health and Human Services regarding related threats which may pose a risk to U.S. health care.

What follows is context on the current cyberthreat environment, along with resources and steps hospitals and health systems can take immediately.

BACKGROUND

There are three concerns for the field, each stemming from the possibility that Russia/Ukraine geopolitical tensions result in increased Russian-borne cyberthreats:

1) hospitals and health systems may be targeted directly by Russian-sponsored cyber actors;

© 2022 American Hospital Association | www.aha.org

2) hospitals and health systems may become incidental victims of, or collateral damage to, Russian-deployed malware or destructive ransomware that inadvertently penetrates U.S. health care entities; and

3) a cyberattack could disrupt hospitals' mission-critical service providers.

AHA's concerns are heightened by the Russian military's previous behavior of utilizing cyber weapons in support of military actions against Ukraine; such behavior ultimately inflicted disruptive collateral damage to the U.S. health care system, resulting in the U.S. government's 2020 indictment of six Russian military intelligence officers for the development and deployment of the destructive NotPetya malware three years prior. The malware was initially launched against Ukraine and subsequently spread globally, disrupting operations at a major U.S. pharmaceutical company, a major U.S. health care communications company and U.S. hospitals.

RESOURCES

The AHA has served as a platform to amplify and provide guidance related to recent government warnings and advisories:

- The AHA on Jan. 28, 2022, received an FBI request for information regarding Russia's recent buildup of armed forces along its shared border with the Ukraine.
- CISA Jan. 16 issued an advisory on destructive malware identified on networks in the Ukraine and to take action to strengthen their networks against potential cyberthreats.
- The AHA and the Health-Information Sharing and Analysis Center Jan. 14 issued a joint advisory strongly recommending organizations identify, and consider blocking, any direct or third-party business associate connections and email contacts based in the Ukraine and that region of the world.
- The FBI and National Security Agency on Jan. 11 released recommendations to help health care and other critical infrastructure organizations prevent, detect and respond to common Russian state-sponsored cyberthreats.

WHAT YOU CAN DO

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

- Hospitals and health systems should review the above-identified 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, 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.

- 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.

© 2022 American Hospital Association | www.aha.org