Hughes Hubbard & Reed

"Shields Up": What You Should Be Doing to Prepare for Russian Cyberattacks

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

February 24, 2022 - President Biden has condemned Russia's invasion of Ukraine and imposed new economic sanctions on Russia. At the same time, U.S. government officials warned of the potential for retaliatory cyberattacks. In addition to the "shields up" advisory previously issued by the U.S. Cybersecurity and Infrastructure Security Agency ("CISA"), the Department of Homeland Security noted this week that "every organization in the United States is at risk from cyber threats" and urged businesses to bolster their cyber defenses.

There have already been reports of Russian cyberattacks against Ukraine. Last week, the United States and the United Kingdom accused Russia of disabling Ukrainian governmental and banking websites. There is concern that such attacks may continue and, if history is any guide, cyberattacks on Ukraine do not stay in Ukraine.

In 2017, Russian intelligence services launched the "NotPetya" cyberattack on Ukraine, deliberately targeting Ukraine's energy sector. However, the malware soon spread out of control, affecting businesses around the world, such as Danish shipping giant Maersk, U.S. pharmaceutical company Merck, the law firm of DLA Piper, British chocolatier Cadbury, and prophylactic-maker Durex.

Businesses need to be preparing now. We list below some simple and immediate steps that businesses can take to protect themselves from potential attacks – whether from Russia or other, opportunistic hackers who may seek to take advantage of the current situation.

- Review your cyberattack response plan. If you do not have a plan, designate a person in charge, with responsibility for coordinating the company's response to a cyberattack.

Also, and specifically per CISA, IT departments should consider the following:

- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls.
- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by anti-virus/anti-malware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.
- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.

The goal is to improve cybersecurity and resilience as quickly as possible. If the crisis in Ukraine continues to escalate, there may not be time to take longer term or more sophisticated measures. Those can come later once the current crisis has passed.

If you require any help or guidance, Hughes Hubbard's cybersecurity team stands ready to help.

Related People

Seth D. Rothman

Kevin T. Carroll

Related Areas of Focus

Data Privacy & Cybersecurity