Shields Up: 10 Proactive Steps Employers Can Take to Prevent Russian Cybersecurity Attacks

Insights
2.24.22

Tensions have been heightening in the Russia-Ukraine crisis given the Russian military invasion that took place late last night – and while this conflict seems to be thousands of miles away, its effects on your business could ripple closer than you may think. Federal cybersecurity officials have issued warnings to American businesses that you should have your "shields up," as Russian cyberattacks against U.S. interests are all but certain to be launched in the coming days. What are the 10 steps you can take today to prevent these malicious attacks on your business, and what should you do if you fall victim?

Digital Warfare on American Soil

President Biden has condemned Vladimir Putin, calling his recent moves an unprovoked, unjustified attack on Ukraine, and has pledged additional sanctions against Russia. Today, Putin issued threats extended beyond Ukraine to "anyone who would consider interfering from the outside," warning that "if you do, you will face consequences greater than any you have faced in history."

The United States is taking these threats seriously. The Department of Homeland Security has cautioned that Russia may retaliate against the imposition of further sanctions by way of cyberattacks launched against U.S. businesses. Likewise, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned of the potential for Russia to launch cyberattacks "outside of Ukraine."

Earlier this week, Secretary of State Antony Blinken stated that Russian cyberattacks are "certainly part of their playbook" and that the United States has been focused on bolstering its cyber defenses "in anticipation of the possibility that Russia would engage in cyberattacks in response to us standing up to their aggression." Further, it was reported that the FBI Cyber Division, in coordination with the FBI's Office of Private Sector, recently issued a report cautioning the private sector that threats of Russian state-sponsored advanced persistent threat (APT) cyber activities are heightened while tensions with Russia are high. The Report directly noted the imposition of sanctions could potentially "increase the volume/severity of Russian APT cyber activities."

What Does Modern Warfare Look Like for American Businesses?

Modern warfare has evolved beyond local, on-the-ground, physical conflict as Russia has proven that its cyber capabilities span worldwide. Recently, Russian hackers have been linked to numerous cyberattacks on Ukraine, including reported mass distributed denial of service (DDoS) attacks this week coinciding with Russia's invasion of Ukraine. And other events have demonstrated that the United States is not off limits. Last year, suspected Russian hackers were successful in launching a ransomware attack which resulted in the shutdown of the Colonial Pipeline, one of the largest pipelines for refined oil in the U.S.

In the past, Russian APT actors have been known to deploy spear phishing, credential harvesting, brute force/password spray techniques, and known vulnerability exploitation against networks with weak security. These cybercriminals exploit unknowing employees, simple passwords, and unpatched systems, in order to acquire access to the existing networks to subsequently initiate persistence and to acquire and steal company data. These hackers have been successful in infiltrating cloud-based networks and enterprises such as Microsoft 365, and have utilized malware in order to extricate sensitive data from these networks.

10 Steps You Should Take Today to Get Your Shields Up

U.S. financial institutions, government contractors, and critical infrastructure sectors, such as electric utilities, are on alert for any Russian activity. However, a "shields up" warning has been issued to *all* U.S. businesses to protect against potential cyberattacks. In light of these threats, it is wise for US employers to take the following steps today to shore up all cyber defenses.

1. Maintain **remote access vigilance**, especially in light of the multitudes of workers who continue to work remotely;
2. Require **multifactor authentication** to access internal network;
3. Keep **security software up to date** and institute timely patching of systems;
4. Enable **robust spam filters**;
5. Enforce **strong, unique passwords** with multiple characters (including numbers, letters, and symbols) and require that they be routinely changed;
6. **Encrypt data** at rest and in transit whenever possible;
7. Implement robust **cybersecurity user awareness and training** programs for new workers upon hire and at least annually for existing employees;
8. Immediately **disable credentials** upon employee departure;
9. Create **data backups** with regularity; and
10. Ensure you have **a strong cybersecurity team** in place to not only monitor your network for vulnerabilities and any suspicious activity but also to develop and deploy an incident response plan (which should include response and notification procedures) in the event of a compromised system.

What Should Your Business Do If You Fall Prey to an Attack?

If your company becomes the victim of a cybersecurity attack, your cyber-incident response plan should be immediately deployed to take the following steps:

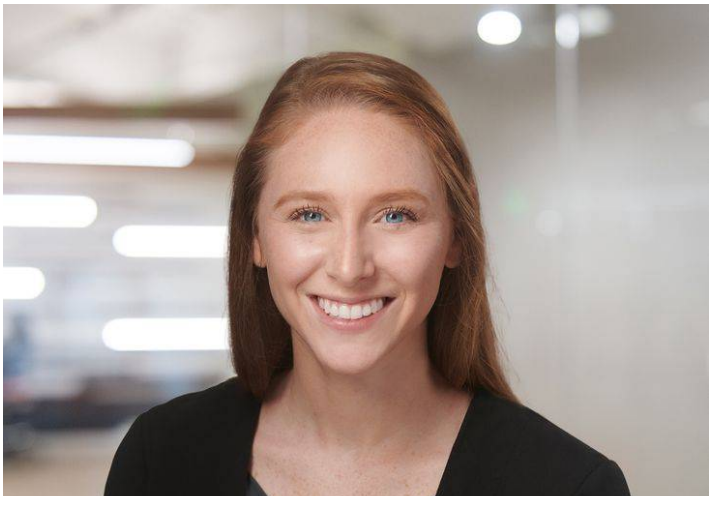
- determine which systems were impacted and immediately isolate them;
- if affected devices cannot be removed from the network (or if the network cannot be temporarily shut down), power infected devices down to avoid further spread of the ransomware infection;
- triage impacted systems for restoration and recovery;
- engage your internal and external stakeholders;
- consider retaining a third-party incident response provider with experience in data breaches; and
- notify affected individuals and report the incident to your local FBI field office.

Companies that become victim of a cybersecurity attack should also hire legal counsel with data breach experience to provide advice on potential notification obligations and to ensure compliance with reporting requirements, as well as to engage appropriate vendors to assist in investigation of the incident.

Conclusion

Fisher Phillips will continue to monitor any further developments in this area as they occur, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information. If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for mitigating the risk of those threats, please consult your Fisher Phillips attorney, the author of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group.

Related People



Ivy Waisbord
Associate
610.230.6108
Email

Service Focus

Privacy and Cyber