Cybersecurity Threats: What Are You Doing to Protect Your Organization?

September 29, 2022

A massive explosion of ransomware attacks in 2021 – 227 million in the U.S. alone – brought into stark realization the magnitude of the cybersecurity threat that has evolved worldwide. A multi-day shut down of the world's largest meat processor, JBS of Brazil, temporarily disrupted global meat supplies and signified the vulnerability of the world's food supply as cybercriminals become more sophisticated. The geo-political upheaval due to the Russia – Ukraine conflict has further clouded the cyber waters.

Certain industries are targeted more frequently than others – financial services and

healthcare being the most impersonated industries in phishing schemes – but no one is immune. Financial services is the industry leader in insider threats and the average cost of cybercrime for financial services is 40% higher than all other sectors.

Many organizations have learned that the “tools rich” environment has not worked. Budgeting for more software tools doesn’t guarantee that you won’t be compromised. What they’ve found out is that they’re resource poor. We believe you need to go on the offensive.

Hunt the Hunter™

To effectively guard against a cyber intrusion, you need to go on the offensive and Hunt the Hunter™. Offensive cyber security strategies preemptively identify vulnerabilities and security weaknesses before an attacker exploits them. Offensive cyber security teams actively test the network’s defenses and provide valuable insights into an organization’s cyber security posture.

Several key measures must be part of an effective cybersecurity protocol, most of which are performed by outsourced cybersecurity consultants:

Vulnerability testing. This identifies vulnerabilities in a system that would allow cyber attackers to gain entrance to your computers, servers and data. Vulnerability testing often yields lengthy complex reports that overwhelm business owners who can’t figure out where to put their cybersecurity dollars first.

Penetration testing. This involves trying to break into your own system, a process that quickly helps prioritize the safeguards that should be implemented first. That’s because it shows exactly which window the cyber attackers can pry open to gain entrance to your system.

Threat hunting. This is a search for footprints often found at an end point where your system connects to the internet. Detection tools are used to examine data flow in and out of the system. The tools examine those persistent mechanisms on servers and workstations that can yield information, such as repeated contacts by IP addresses in certain foreign countries.

Threat intelligence. Developing an overall understanding of what attackers are doing in your industry is an essential part of cyber security.

Some states, including New York, require financial services companies to do regular penetration testing. But the law only requires a basic level of testing that may not keep all organizations safe.

How Can We Help?

The cyber threat is only growing, and the time for relying on software tools and operating system patches is in the past. Anchin's affiliate, Redpoint Cybersecurity, can perform a **Cyber Posture Assessment** that will provide you with actionable intelligence about your organization's security operations program, as well as an in-depth assessment of your overall breach readiness. From examining configured operating systems, to identifying the misconduct and misconfiguration of services, to browsing, to applications, to password management policy, and many additional indicators – we will arm your team with a complete, organization-wide view.

We are always here to help. If you have any questions, please reach out to Anchin's affiliate, Redpoint Cybersecurity's Russell Safirstein, President & CEO, or your Anchin Relationship Partner.