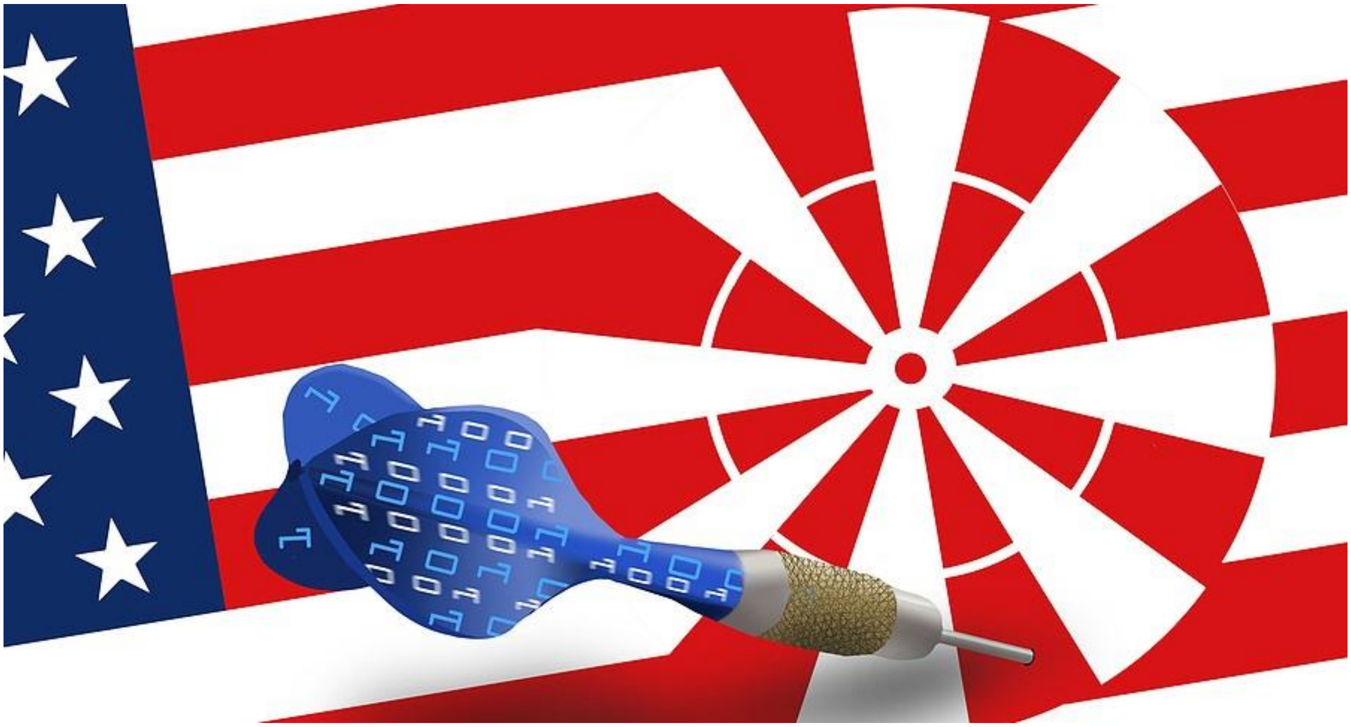
State-backed Cyber Attacks Pose Dangerous Threat to Business



In late 2020, a study showed that 80 percent of businesses worried about state-backed cyber attacks. Within weeks, the Russian-sponsored SolarWinds hack and the China-backed Microsoft Exchange hack came to light, confirming those concerns. Should businesses and individuals fear these attacks, or do they only affect government agencies?

Lawless Frontier Invites Multiple Players

In recent years, countries have increasingly turned to the cyber arena to conduct espionage and warfare. Unlike traditional warfare, very few international laws exist to govern cyber warfare. And, while Russia and China currently dominate the stage, smaller countries can also make a big impact with a relatively small investment.

Typically, state-backed cyber attacks accomplish one of three main goals. As the United States has discovered, foreign nations use cyber warfare to interfere politically by spreading misinformation. Additionally, these attacks allow countries to conduct espionage and benefit financially.

No Business Immune from State-backed Cyber Attacks

While movies make attacking government agencies look relatively easy, these agencies generally employ extremely robust security. In the business arena, however, executives too often prefer to deflect funds away from cybersecurity to areas that directly affect revenue. Consequently, businesses make attractive targets to achieve key goals.

Hence, the susceptibility to attacks comes down to the value of the organization to the attackers for political or financial benefit.

For instance, if hackers conduct a successful attack against an organization that provides electricity, telecommunications, or other critical services, they can cause widespread disruption. Likewise, businesses that hold government contracts may store extremely sensitive and valuable information.

Other high-profile targets include institutions that cannot afford IT downtime and will thus prove more likely to pay ransoms. Additionally, the COVID pandemic has given rise to attacks on makers of COVID-19 vaccines. And the rapid increase in remote work related to the pandemic has also exposed new attack vectors.

Protecting Your Business

In many respects, state-backed hackers use the same tactics as other common cyber attacks. Phishing schemes, denial-of-service (DDoS) attacks and man-in-the-middle operations are especially popular, for example. However, these attacks generally present an unusually high degree of sophistication, run by well-educated and well-equipped engineers.

To counter such attacks, consider the following cyber security tips:

- **Build on a foundation of basic cyber security best practices** – Resist the temptation to cut corners on basic security measures. For example, apply security patches quickly, ensure encryption, conduct regular backups, and deliver regular security training to employees.

- **Isolate critical systems, where possible** – When feasible, segment your network to protect sensitive data assets. That way, even if hackers do breach the system, they will have difficulty accessing key intellectual property.

- **Audit your supply chain** – Conduct regular infrastructure audits to identify all hardware and software involved. Make sure you know what third parties have access to your system and how they gain entrance.

- **Collaborate with others in your industry** – Share threat intelligence with other organizations that operate in your market space. Fighting against state-backed hackers requires a group effort.

- **Adopt a proactive, rather than reactive, security posture** – Do not wait until an attack occurs to address cyber security. Instead, use the past as a starting point for addressing weaknesses. Additionally, conduct phishing simulations regularly and in other ways focus on anticipating and preparing for the likely direction an attack will take.

Security Partners Offer Peace of Mind

When facing a dangerous enemy, you need powerful allies on your side that deliver multiple layers of protection to keep the organization from risk. Partnering with proven security experts takes the guesswork out of creating an effective cyber security strategy.

The security specialists at Messaging Architects make it their business to stay abreast of both current threats and the cyber security strategies to counter them. They will conduct a comprehensive risk assessment and work with you to tailor a security plan to your needs and budget.