AIM

AIM CYBER

High-touch services to help you navigate modern cyber threats.

CYBER THREATS AFFECT EVERYTHING

Supply chain threats are a new attack pattern that causes devastating results. SolarWinds was the first one discovered. But now we know that other software suppliers have also been infiltrated.

These attacks are especially insidious because they affect and infect so many companies. But what is most concerning is the deviousness of the attack.

Nation-state actors are thought to be behind these attacks. That adds to the concern because nation-states have deeper pockets than cybercriminals and can afford to play the long game. Cybercrime is a way to cause devastation without conventional warfare. Of course, nation-states deny responsibility because determining the source of the infections is not easy.

And without armed troops in uniform, it is easy to deny responsibility. The identification is often done by comparing the infection to other known infections.

What does all this mean to companies? Good question. The short answer is nothing can be considered safe. Software distributions can no longer be considered malware-free.

Emails, attachments, web downloads, all have been scanned routinely. Or at least should be scanned routinely as part of good cyber hygiene. But software updates were accepted as clean and safe. Recent events show that is no longer the case.

Vendors certainly need to do their own testing before distributing an update or a new software product. Now it is necessary to scan and test everything. Even hardware products need to be scanned and tested before distribution as they have software inside and will go on a company or home network.

As much as possible, everything should be scanned. The Zero-trust approach now includes new software.

There was little considered safe before these supply chain compromises, now there is less.

It is easy to assign blame but that won’t help restore your systems or resecure stolen information and the NPI, non-public information, of your customers, clients, or patients.

Remember, cybercriminals are always looking for new weaknesses to exploit. Until the first exploit occurs, the weakness may not be known. Until it is known, it can’t be fixed.

Cyber security is everyone’s job. With no exceptions. Training is essential as is reporting suspicious emails, messages, texts, and activity to your cyber security team. This may not catch everything, but it will catch many of the attempts at compromise.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.