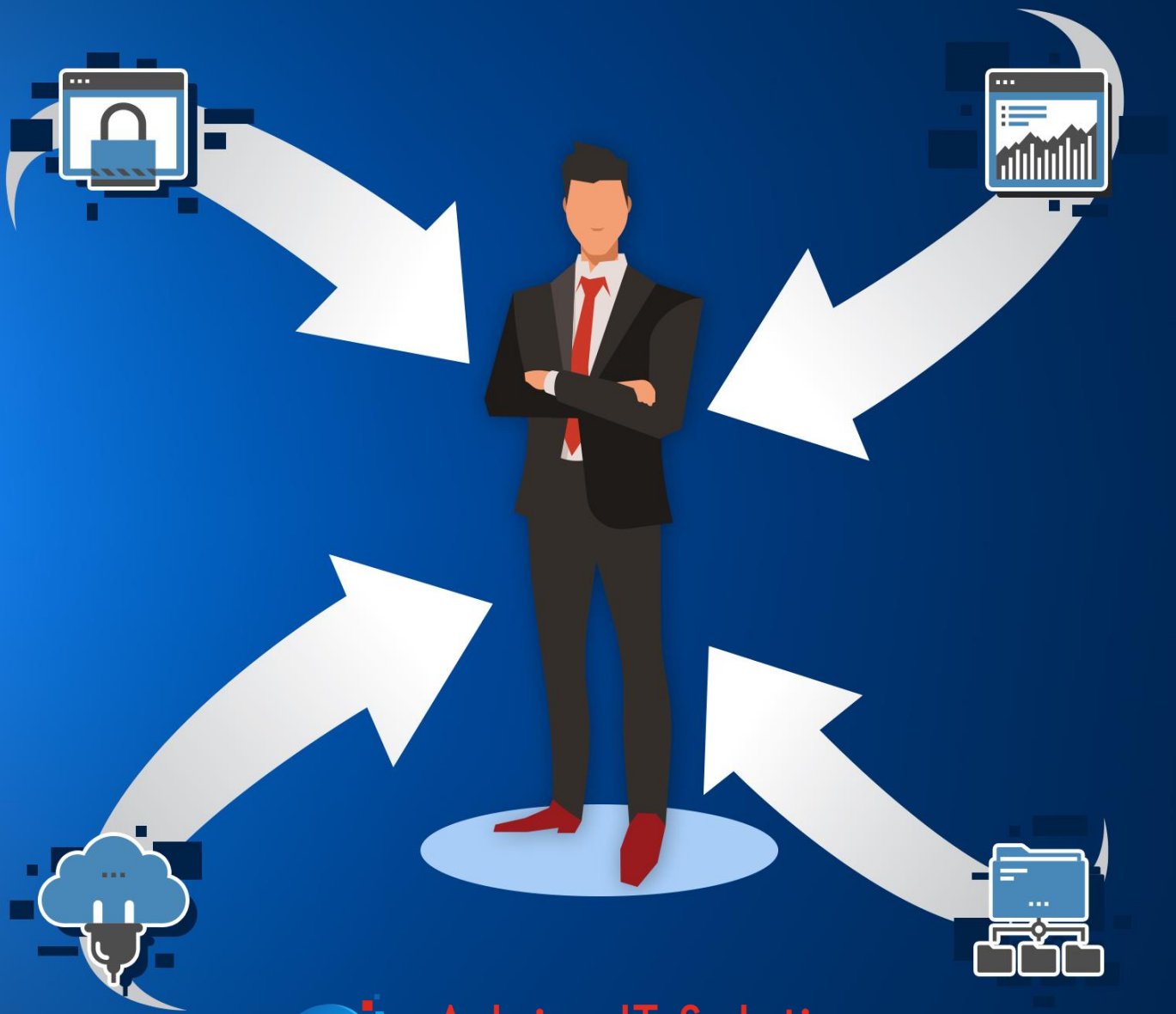
5 THINGS YOU NEED TO KNOW ABOUT SUPPLY CHAIN ATTACKS



Advise IT Solutions

Productive IT.

Supply-chain attacks may not grab the headlines in the same way as ransomware or data breaches, but these sneaky cyberattacks are just as dangerous for your business.

This eBook explains five things you need to know about supply-chain attacks, including what they are, why they happen, and how to prevent them.

Thinking of a supply chain, you envision taking raw materials to finished product. The process might start with cows and end with milk. The supply chain covers refining, manufacturing, packaging, and transportation. Yet supply-chain attacks in the IT sense are much more than tipping those cows in the farmer's field. These cyberattacks see bad actors targeting vulnerabilities where businesses connect to one another. A supply-chain attack exploits a weakness at the target company's vendor.

In one well-known example, hackers stole 40 million financial records from a brick-and-mortar retailer. The hack caused Target's company profits to fall by 46 percent after they announced the news. The attackers did not start with Target directly. Instead, they used credentials stolen from a heating and air conditioning provider.

A supply-chain attack can occur in any industry. In fact, the problem is only getting worse as businesses grow.

more interconnected. Here are the top five things you need to know about supply-chain attacks to prevent and protect.

#1. What is a Supply Chain Attack?

At its most basic, a supply-chain attack is opportunism. This type of attack is also known as a value-chain or third-party attack. It occurs when someone gets into a system through access to a supplier or service provider.

Instead of attacking the enterprise, the cybercriminal targets the weakest link. As businesses become more interconnected, the attack surface grows larger. Try to find a business today that is not providing network access to a software vendor, payment processor or cloud backup solution, or that is not using installed applications and connected devices. A compromise at any one of these could give a bad actor access to your business network.

#2 What Makes Supply-Chain Attacks So Dangerous?

For one, they can happen to any business. From critical infrastructure entity to financial services firm, every business connects to supply-chain partners. The complexity of IT compounds attack risks. Many business owners do not know how the integration works but simply trust that it will.

At the same time, software developers often rely on open-source coding components. This is what makes modern application development affordable and agile. Yet reusing code means that a vulnerability, once found, can be exploited in many different scenarios.

Supply-chain attacks are especially effective because they leverage a legitimate connection. Besides all the business software, there are connected routers, servers,

Internet of Things devices, mobile phones, and computers, too.

Additionally, the hackers can often hit many businesses at once. Since a supply-chain vendor stores data for more than one client, the attack can lead to many victims.

#3 Why Are Supply-Chain Attacks Growing?

According to a study by Symantec, supply-chain attacks increased by 78 percent in 2019. Why? Relying on third-party solutions is common in business. Digital transformation is reshaping how we do business. An integrated supply chain is more efficient, productive, and cost effective. Plus, with digital data, decisions are based on information rather than gut instinct.

Yet cybercriminals do not sit and stagnate. A business process supply chain means more people need access to sensitive data, and that shared access is a viable vector of attack for the bad guys.

They have greater odds of getting in via the small business. Running at a high-value target is a little like trying to take down a steel door with your shoulder. But, if you can run at a small business with access to the real target, it is a lot more like kicking in a door made of paper. That smaller entity provides a vital service but lacks the skills and resources for impermeable defence. The criminal uses this to find insecure devices or mine credentials needed to attack.

Still unconvinced supply-chain attacks are a big deal? In May 2021, President Joe Biden of the United States instituted an Executive Order. One section was devoted to supply-chain attacks.

#4 How Do Supply-Chain Attacks Happen?

There are many ways to breach a supply chain. The top three methods are:

- exploiting networking vulnerabilities.
- leveraging unpatched software.
- social engineering.

No one is going to let a supply-chain attacker in on purpose, but small businesses might be slow to update software and antivirus protection. Without the latest protection against formidable threats, the business is at greater risk.

A business relying on legacy software or equipment can also be vulnerable. With budgets tight and processes working fine as is, the business might resist upgrading. Yet, using an operating system after its end-of-life is risky. The manufacturer has stopped offering support and security updates.

Another means of supply-chain attack is through devices with pre-installed malware. This might be a USB drive or another physical device that connects to the company's infrastructure. The Stuxnet worm that infected an Iranian nuclear plant was delivered on a removable thumb drive.

Open-source software is another possible threat. A 2017 breach at Equifax cost the credit reporting company nearly $2 billion. The hackers preyed on an unpatched vulnerability on a consumer complaint portal.

#5 How Can You Guard Against Supply-Chain Attacks?

Vet your vendors. There is a lot of cheap, convenient software out there, but you will be better off paying for a thoroughly tested solution. More businesses today

assess third-party risk using questionnaires and documentation reviews.

You cannot simply trust that your business partners are as determined to secure their network as you are. Ask vendors to write down what security controls they have in place and how they manage risk. This will help you see they are taking cybersecurity seriously. Plus, you can identify whether their actions are compatible with your own.

Consider compliance. Insist that partners have standards of care regarding cybersecurity. Depending on your industry, you may also have regulatory frameworks to comply with. Make sure all parties in the supply chain are compliant and test their security posture.

Limit access. When you do enter a partnership with a third-party, be sure to limit their access. Use the least-

privilege approach. This means the vendor has permission to access only pre-determined sites or systems. This helps prevent software from communicating with malicious command and control servers. Plus, set up alerts for third-party credentials used to do something out of the ordinary.

Know your inventory, not on your warehouse shelves but the inventory of connected devices on your network. Do an audit to get a full list of all open-source and other types of software, hardware, and systems. Once you have this, replace, or stop using any outdated systems, services, or protocols.

Remove unapproved IT. You tell your employees not to download unauthorized apps onto your IT infrastructure, but they prefer certain software. Or it makes their lives easier, so they do it anyway. Root out any unapproved IT – also known as shadow IT – as it puts your business at risk.

Deploy patches. Your business needs to have patch management and software update processes in place. Do not ignore that notice to install the latest version of a system planning on catching up on the next one. You could be missing out on plugging a gaping hole that the manufacturer has found and fixed.

Keep up with vulnerabilities. according to IBM, third-party vulnerabilities caused 16 percent of all data breaches in 2020. These attacks are a sneaky way to get the job done. Follow industry news and track cybersecurity notifications from industry and government agencies. Your business must make sure it is aware of the risks and is doing its best to cut them.

Support Against Supply-Chain Attacks

Supply-chain attacks are a daunting problem. Do not worry. Your business does not have to do it alone. Our IT experts can tackle the to-do list and help guard your systems against supply-chain risks.

Complacency is not the answer. Regardless of industry, or business size, you could be rocked by a supply-chain attack. Take proactive action to prevent the worst. We can help. Contact us today at (951) 777-2004.

Advise IT Solutions

Productive IT.

Phone: **(951) 777-2004**

Email: Hozi@AdviseITSolutions.com

Web: www.AdviseITSolutions.com

Facebook: https://www.facebook.com/AISManagedIT