https://www.wsj.com/articles/more-side-door-hacks-are-coming-here-is-how-businesses-can-prepare-11614096250

THE EXPERTS | LEADERSHIP

More ‘Side Door’ Hacks Are Coming. Here Is How Businesses Can Prepare

The SolarWinds attack wasn’t the first so-called side-door hack and it likely won’t be the last, says WSJ Leadership Expert Stuart Madnick.

PHOTO: GETTY IMAGES/ISTOCKPHOTO

By

Stuart Madnick

Updated Feb. 23, 2021 11:18 am ET

Stuart Madnick is the John Norris Maguire Professor of Information Technologies at the MIT Sloan School of Management and the founding director of the Cybersecurity at MIT Sloan (CAMS) research consortium.

The hack of SolarWinds Corp. , a maker of network-management software, has been called a “game-changer” due to its breadth and success. Hackers planted malware in a software update that SolarWinds sent out to its customers, affecting as many as 18,000 organizations, including the U.S. departments of Homeland Security, Commerce and Treasury.

While many experts say the complexity of the attack represents a new frontier for cybersecurity, it also is the latest episode in a continuing game known as the “side-door hack” that some companies aren’t prepared to play.

THE EXPERTS

The Experts are a group of industry and academic thought leaders who weigh in on topics covered in the The Journal Report.

The technique of attacking an organization through a trusted vendor isn’t new. It happened in 2013, when hackers used the stolen credentials of a contractor working with Target Corp. to breach the retailer’s computer network, and again in 2017, when hackers planted malicious code in the updates to a tax program sent out by a small Ukrainian company, Linkos Group, leading to the NotPetya cyberattack that crippled the computer networks of multinational companies world-wide.

So what can organizations do to protect themselves before the next round of the side-door hack game starts? Defense comes in two forms: prevention and mitigation**.** Both must be addressed.

Prevention: An organization should carefully evaluate the quality of a vendor’s cybersecurity before giving that vendor a “pass” to its network. If an organization can’t perform a security audit on its own, there are firms that specialize in providing such audits or ratings. Should a vendor with an “average” rating be trusted? That depends on a business’s security needs, and it will vary by industry. Security audits have an added benefit in that they provide a tangible incentive for vendors to improve their cybersecurity.

Mitigation: If malware gets into an enterprise, the damage can be reduced with faster detection, de-escalation and data-exfiltration restrictions.

Faster detection: Various studies have shown that dwell time—the time between when an intruder gets into a system and when the breach is discovered—averages around 200 days. Why isn’t it noticed? Often, no one is looking. Big mistake!

There are many ways a cyberattack in progress can be recognized, including unusual password activity, suspicious pop-ups and slower-than-normal network speeds. The SolarWinds hack was discovered by cybersecurity firm FireEye Inc. , a SolarWinds customer. FireEye launched an investigation after receiving an alert about the unauthorized use of an employee’s credentials, eventually finding the “backdoor” code in the SolarWinds software.

Minimizing escalation: Companies should take steps to restrict how far malware can travel through their systems. One approach, called “zero trust,” is based on the principle of “never trust, always verify.” Among other things, that means limiting access to the most sensitive parts of a network only to people in certain roles or those who need to be there. Unfortunately, too many companies run their software like an “open space” office, with no doors or offices, even the areas that have critical data. That gives intruders free rein to easily move into increasingly important areas of a company’s computer network and data storage.

Restricting data exfiltration: Probably the most obvious, though frequently neglected, mitigation strategy is exfiltration detection and restriction. If a bank teller left work every day with a wheelbarrow full of money, those running the bank would surely notice. Similarly, companies need to monitor the data traffic leaving their networks. Most computer systems make logs of all key activities, such as users logging in and data being sent out. Tools are available to help companies analyze these logs in real-time, making it easier to stop data exfiltration almost immediately or at least daily. At the very least, this might prevent hackers from lurking on a network unnoticed for 200 days or so.

Hackers are quick to duplicate successful attack methods, so this is unlikely to be the last “side door” attack we see. Companies need to prepare by taking action now.

You can email Mr. Madnick at reports@wsj.com.