TechTarget: 5 cybersecurity lessons from the SolarWinds breach

written by Nabil Hannan | February 8, 2021

On February 8, 2021, NetSPI Managing Director Nabil Hannan was featured in TechTarget:

Ransomware attack simulations, accessing enterprise logs and pen testing software code are among the best practices cybersecurity pros suggest following the SolarWinds breach.

Forensics teams are still investigating how hackers were able to exploit SolarWinds' patching system to attack numerous high-profile commercial and governmental organizations, including Microsoft and the U.S. Department of Justice, as well as other customers of the security monitoring software vendor. At the same time, experts from a range of security service providers – including those offering penetration testing, vulnerability scanning and software code reviews – advise businesses to act now to shore up their own enterprise security.

The SolarWinds breach was first revealed in late 2020 – although the attacks may have begun in 2019 – and now includes the discovery of two backdoors created by malware. The first, named Sunburst, has been linked to numerous supply chain infections and nation-state attacks, and the second, named Supernova, is not a supply chain attack, but rather malware that required the exploitation of a vulnerability in the Orion software program recently patched by SolarWinds. U.S. government and cybersecurity experts are still uncovering the damage caused by the two infections.

Security service providers suggest the following list of five lessons learned to help organizations ward off or detect a SolarWinds-type hack. These best practices also lessen the "threat noise" across the enterprise, enabling a company to quickly identify and handle suspicious behavior.

Don't rely on internal developers to test internally developed software

Developers should not have the final say on how secure their code is. They are not security experts, and they might be the ones who inserted malicious code, intentionally or not, according to Nabil Hannan, managing director at pen testing provider NetSPI. "To uncover a SolarWinds type of issue, you have to think differently than a developer would about what you are looking for, including who has access to your systems," he said. "How can a developer determine another developer's true intent for putting code in the system and how it will behave? He can't." Hannan recommended forming a group of trusted executives and senior managers to work with an external testing firm. When developers are done with their reviews or completed updates, the group sends it to the testers to look for malicious code and insider threats. "We examine the source code and binaries, looking at executables

and comparing what is published versus what is in the source code," he said. Testers search for backdoors, time bombs, Trojan horses and signature patterns. "If there are differences, we will report back to the group in a discreet way and work with them to mitigate the issues." Hannan said having this practice and these controls in place are helpful when there is a management shakeup, a disgruntled developer leaves or a merger or acquisition is about to take place.

Read the full article here: https://searchsecurity.techtarget.com/feature/5-cybersecurity-lessons-from-the-SolarWinds-breach