SolarWinds says its new security measures are reassuring clients

March 29 2022, by Gopal Ratnam

Credit: CC0 Public Domain

SolarWinds says it has beefed up security and tightened its software screening process 15 months after one of the most sophisticated cyberattacks exposed thousands of its customers to Russian spies and left U.S. government agencies and Fortune 500 companies scrambling to contain losses.

SolarWinds executives say they have spent $25 million to improve

security and established new processes to screen third-party code that goes into almost all software products.

The company now operates on the principle of "zero trust and assuming breach mentality"—tech-speak for taking as a given that security breaches are inescapable—said Chip Daniels, the head of government affairs at SolarWinds.

The company also has instituted a process requiring all software be built in triplicate by separate teams to prevent malware infections because of loopholes or deliberate mischief, he said.

Outside software developers are being subjected to a screening process that requires them to "answer a series of questions that will assure us that their environment is secure," Daniels said.

In December 2020, cybersecurity research firm FireEye revealed that network management software made by SolarWinds had been breached, potentially exposing as many as 18,000 of the latter company's clients.

In-depth assessments revealed that of those clients who were likely to have been exposed, only 100 were affected, the company has said.

U.S. officials later said the attack was carried out by Russian intelligence operatives who broke into a software update process used by SolarWinds and used that to gain access to clients who had unwittingly installed the tainted software update.

In the immediate aftermath of the attack, U.S. officials asked all federal agencies using SolarWinds to disconnect the software and rebuild their computer operating systems. Cybersecurity experts feared that Russian spies might have placed secret backdoors that they could access later.

The new measures are causing federal agencies that feared using the company's software to reconsider, Daniels said. But he declined to name the agencies because negotiations were still underway.

The company is reassuring its old and new customers that it has undertaken a comprehensive security review to find and remove any remnants of the Russian attack, said Tim Brown, chief information security officer at SolarWinds.

The company worked with federal agencies, including the FBI and the Cybersecurity and Infrastructure Security Agency, as well as private cybersecurity firm CrowdStrike and forensic auditors from KPMG for six months "looking and hunting, examining for any anomalies we might see" in the software, Brown said.

The company examined every software code going back two years and found no anomalies, Brown said.

Although the Russian attack did not stem from an insider threat, it "doesn't mean it couldn't happen next time," Brown said. To prevent such an outcome, the company adopted the "triple build" model of software development, he said.

One version is built by developers, while a second one, called the validation version, is simultaneously under development, and a third security version is also developed, Brown said. Before shipping out a software update to customers, the company compares the three versions to ensure they are identical, he said.

The new approach ensures that any attempts to inject malware "you would need to have collusion amongst at least three people," which is far less likely, Brown said.

Since software, like most physical products, is assembled with inputs from a global list of suppliers and draws on open-source components, SolarWinds now uses a set of seven questions to screen the security measures adopted by its suppliers, Daniels and Brown said.

The questions include a detailed breakdown of each supplier's software development process, how suppliers secure their physical and electronic infrastructure, their risk management practices, how they respond when a breach or a vulnerability is discovered, methods used to identify internal threats, how they validate changes to their software code and how they screen new employees to identify potential foreign actors.

The questions were built off of the first set of questions CISA asked SolarWinds in the immediate aftermath of the attack, Brown said.

The company now recommends that other software developers use the screening questionnaire to assess the security of their suppliers, Brown said.

SolarWinds also is building a database of all the software code that goes into its products in order to develop a so-called software bill of materials, Brown said.

In May 2021, President Joe Biden issued an executive order on improving cybersecurity measures across the federal government and private companies. One of the elements of the order called for software sellers to provide buyers with a software bill of materials.

The order said the bill of materials refers to "a formal record containing the details and supply chain relationships of various components used in building software."

Brown said in some cases the bill of materials could run to tens of

thousands of pages and could overwhelm customers trying to evaluate a vendor's offering.

SolarWinds, like other software companies, is working to make the idea of bill of materials practical and useful to customers, Brown said.