Two Key Factors That Impact Software Security

Is your product software really as secure as you think it is? Most companies and developers would probably say yes, but the reality is quite different. There are hidden security threats lurking within products and networks all over the United States. This is one of the reasons that the FBI Director and others have been expressing security related concerns for over a year. We all want and strive to build security into our solutions. However, common engineering processes are making that extremely difficult. And what you don't know, will hurt you, government networks, and American businesses.

The problem is very clear. Over the past several years, there has been a focus on hardware security. However, less attention has been paid to software security. This has led to both direct and indirect damage to American businesses. For instance, the September 2019 SolarWinds hack is an example of a direct security attack by nefarious individuals. An example of indirect damage was the July 2024 CrowdStrike outage caused by errors in CrowdStrike's software validation process that crippled millions of United States and worldwide computers. Both are examples of how reliant our computer systems are on software operation.

There are two fundamental security risks with most software products today:

1 An over reliance on open-source software

2 Extensive use of foreign software programmers and foreign software manufacturers

Open-source software is an attractive option for both financial and technical managers. It's cost-effective and can deliver a faster time to market than self-development of software. However, product and customer security risk increases dramatically with this choice. You assume that the libraries and code you use have been tested by others. But how good did they test the code and look for problems? If the verification work is not done properly, you can end up with a situation like the CrowdStrike outage.

In addition, you can end up with a situation where you use well-known libraries, like Node.js, only to find out (much later when you're in production and have delivered solutions to customers) that the code is riddled with defects. According to a 2022 Dark Reading article, researchers at Johns Hopkins University reported that they found 180 different zero-day vulnerabilities that were spread across thousands of Node.js libraries. A 2024 Black Duck (Synopsis) study found that 84% of the open-source software codebases that they assessed for risk contained some type of vulnerability. This should be a sobering concern to any manufacturer or any purchaser of software products, i.e. everyone.

A second concern is the increased use of foreign contractors and sub-contractors for software development. Software product design is a highly sensitive and critical component of modern solutions. It is important to know who has created or contributed to the development of the software, especially since a new product will probably connect to multiple other products in an enterprise or military agency. This interconnection creates a serious point of security risk for the entire network.

One area of serious concern is the integrity of software engineers assigned to the product. For instance, is this work done internally by the US company or are parts of the project outsourced to workers in other countries? If the work is outsourced, have those workers been compromised by a nefarious nation state or are those engineers actually nation state actors being paid to infiltrate certain product development teams? Also, is the US-based company using products and solutions from foreign companies that are on the United States government banned list? Understanding the answers to these questions is important not only for the company producing the product but also for any US companies or government agency using those products in their production networks.

A study by Fortress Information Security revealed that a staggering 90% of the software products they reviewed that are part of the U.S. power grid contained components developed by individuals from China or Russia. The Fortress Information Security study also found that “software with Russian or Chinese-made code is 2.25 times more likely to have vulnerabilities.” In addition, ”… that software is three times more likely to have critical vulnerabilities.” It should also be noted that North Korea (according to Security Week) is using hundreds of nation-state operatives to pose as fake remote workers to infiltrate US companies. Part of this is to help North Korea to fund their illegal programs. However, attackers also performed various actions to manipulate session history files, transfer potentially harmful files, and execute unauthorized software.

Overcoming Software Security Risk

The use of open-source and foreign made products has created credible concerns about US national security and data privacy. Despite an increased focus on product security, software security still lags behind. Your best defense against this threat is to buy from domestic companies that develop software domestically by US citizens. Look for companies that adhere to internationally recognized security standards like ISO 9001:2015 and possess relevant certifications, such as the DoD Authority to Operate (ATO).

Contact Axellio and we can show you how to create unparallelled network visibility and optimize your security and monitoring solutions without compromising your network security. We use United States citizen workers and do not overly rely on the use of open-source code. Axellio carefully manages its use of open-source components and rigorously tests and evaluates the code used to reduce exposure to vulnerabilities.

Learn more at: www.axellio.com

Axellio delivers scalable, simultaneous, always-on recording and distribution at over 200 Gbps with no data loss.

For more information, contact us at: www.axellio.com/contact-us/