U.S.
Resilience
Project

Cybersecurity: A New and Growing Threat for Supply Chains

From the McAfee Blog Center
By Dennis Omanoff
November 2, 2011

Before Sept. 11, 2001, most supply chain professionals focused their security measures on preventing the theft of valuable goods in their manufacturing and transportation operations. After 9/11, greater emphasis was placed on preventing weapons of mass destruction — or disruption — from being placed in cargo containers or other conveyances headed to the United States.

Today, there is an even more potentially destructive threat to the supply chain community that is often overlooked. The volume and sophistication of cyber threats from totalitarian governments or nefarious individuals are increasing exponentially. This 21st century threat jeopardizes not only our information infrastructure, including in the supply chain community, but also all levels of high-tech software and hardware products that connect with local or enterprise-wide networks, either hardwired or wirelessly.

Concerns continue to rise about the "injection of viruses" into high-tech hardware products during their journey from manufacturing sources to customer delivery, especially to government agencies. More than natural disasters, financial instability or political upheavals, what keeps me up at night is the fear that bad guys are injecting bad stuff into products that can disrupt, bring down or steal confidential information from networks.

For example, McAfee reviews about 100,000 potential malware samples per day, identifies more than 55,000 new, unique pieces of malware per day, and identifies about 2,000,000 new malicious websites per month. In the past two years, persistent and highly organized cyber attacks such as STUXNET, AURORA, WIKILEAKS, ShadyRAT and NIGHT DRAGON point out how cleverly the bad guys can worm their way into the world's most protected networks and either sabotage them, steal intellectual property, or compromise government trade or military secrets.

Given these examples, how safe are our networked products — from software to computers and servers — and how can we protect their security from component sourcing to the factory to assembly and delivery to the customer?

First, supply chain professionals charged with manufacturing and delivery processes should look beyond traditional threats such as tsunamis, demand volatility or financial degradation and take extra precautions to ensure that technology products, in particular, are safeguarded from viral attacks.

At McAfee, the largest dedicated information security company, a number of strict measures have been put into place to protect and prevent the infection of products, especially hardware-assisted security systems such as firewalls, mail and web security network appliances, risk and compliance, cloud-based networks, and intrusion detection and prevention.

For example, all of McAfee's suppliers must have an information security policy in place for data loss prevention and system control that provides complete protection of both network and host leakage. Today, the adulteration of data or the loss of intellectual property should be center to every company's core risk program, and that includes the supply chain community.

Compromising a company's IP can jeopardize an entity's competitive advantage, cut into market share, and even endanger our customers' reputations, not to mention the vulnerabilities to top secret government information. The sharing of data from McAfee to our suppliers is important for new product development, continuous improvement of our product, elimination of customer issues, and the ongoing growth of product lines.

In addition to strict qualifying standards for its suppliers, we have architected a global supply chain operation where component parts are secured via distribution partners from multiple locations and then assembled, converted into finished products, and shipped by trusted sources chosen by customer preference. Any of our products can be made or assembled from any of our strategic locations in Europe, North America or Asia, and also shipped to any other locations, almost at a moment's notice.

The final assembly and hardware conversion, whether it is software, adaptor cards or some type of interface card, and final shipment can be done very quickly — we aim for 20 minutes from the time an un-forecasted order comes in (aim for 30-day lead time on predictable orders). With this type of sense and respond network, we are able to obfuscate the trail of the quickly assembled final product so that it is nearly impossible to know beforehand where it is headed, whether it is an energy grid, nuclear power plant or government agency.

Further, it is critical to keep as low an inventory and backlog as possible — as the saying goes, "Inventory at rest is inventory at risk." This not only makes good security sense, but also good business sense.

By having a geographically dispersed supply chain and trusted partners that can operate as a single unit, professionals can satisfy the unique requirements of customers in various regions. For example, "Assembled in the USA" verification helps meet stringent U.S. government (and some European government) requirements, but similar in-nation rules and incentives are imposed in other parts of the world, which punctuate the need for highly flexible supply chains.

These different security requirements can be met with what Dr. Hau Lee at Stanford University calls "multi-polar, differentiated supply chains." In other words, complete regionalized supply chains working either independently or as a unified operation can meet localized and globalized customer demands, while also creating an operation that protects products from being sabotaged with the latest cyber virus somewhere along the way.