February 2013

Supply Chain Security

Key Points

- Governments worldwide have concerns about supply chain security, in particular the potential for hostile actors to insert malicious software into information technology products as they move through the supply chain. This could create vulnerabilities in the information and communications technology systems when compromised components are introduced.

- Microsoft employs a four-part strategy to manage the risks to its products and services in the supply chain. This strategy is grounded in identity and access management controls, the Security Development Lifecycle, policies and procedures that monitor the integrity of Microsoft software, as well as anti-counterfeit measures.

- Governments and businesses need to recognize that supply chain security is a shared problem, and that they must work together using risk-based solutions, best practices, and international cooperation.

BACKGROUND

Information and communications technology systems perform an increasingly important role in commerce and in daily life. Some of the more critical systems have become attractive targets for malicious actors who mount increasingly sophisticated attacks that have the potential to cause widespread damage or disruption, or give them unauthorized access to data.

A key area of criminal interest is the supply chain of technology products, which the National Institute for Standards and Technology defines as "the set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers."

The supply chain responsible for delivering information and communications technologies is globally distributed. The products themselves can be complex, made of many parts in many different companies all over the world. This raises concerns about the potential for hostile actors to introduce malicious or unwanted functions or counterfeit elements along the way. If products are compromised, they could potentially be used to conduct surveillance or to disrupt or otherwise degrade the trustworthiness of the information and communications technology systems of which they will be a part.

Securing such a diverse and global supply chain presents a challenge for governments and businesses. Both need to recognize supply chain security as a shared problem and seek solutions that are built upon best practices, mitigate risks, and draw on international cooperation.

MICROSOFT APPROACH

Microsoft's strategy to help mitigate supply chain risk to its products and services includes:

- **Identity and access management controls.** Microsoft uses policies, procedures, and technology that manage personnel access to Microsoft intellectual property.
- **The Security Development Lifecycle** is a foundational element for reducing the risk in the development of Microsoft software, and for protecting it against the introduction of product vulnerabilities, whether malicious or inadvertent.
- **Software integrity controls.** Microsoft employs policies, procedures, and technology to preserve the integrity of its software products, including code signing and checking for malware.
- **Anti-counterfeit measures.** To protect customers from the risks of counterfeit software, which could contain vulnerabilities, Microsoft actively identifies counterfeit versions of its software, works to maintain the integrity of its distribution models, and works closely with law enforcement agencies around the world to help reduce piracy.

Microsoft also takes legal and technical action to address criminal efforts to target the supply chain. For example, the Microsoft Digital Crimes Unit works with other Microsoft teams to fight aggressively against botnets. One such initiative is Project MARS (Microsoft Active Response for Security), which focuses on efforts to disrupt criminal infrastructure. This includes taking legal and technical action to pursue botnets and help undo the damage they cause. In 2012, Project MARS helped take down the Nitol botnet, which infected computers through vulnerabilities in the supply chain.

POLICY CONSIDERATIONS

A framework for managing supply chain risk should rest on these principles:

- **Risk-based approach.** Governments should avoid using simplistic factors such as a product's country of origin to assess risk. The global character of many products means that attempts to prohibit products based upon country of origin could result in a broad ban of products. This would lead to weakening open trade and relinquishing the benefits of global innovation. Instead, governments should rely on tested risk-management principles.
- **Transparency.** Governments have a right to expect IT companies to provide an appropriate degree of visibility into their business processes and the controls that ensure the security of their product development and operations.

  One example of such transparency is Microsoft's Government Security Program, which gives eligible participating governments access to the source code for selected Microsoft products. While expecting transparency, however, governments also need to appreciate that businesses must protect their trade secrets and other intellectual property.
- **Flexibility.** When governments move to adopt standards governing supply chain security, control and mitigation standards need to remain flexible.
- **Reciprocity.** The development of reciprocal international standards for supply chain security is essential for continuing to realize the benefits of the Internet that rely on the security and integrity of information technology systems.

Helpful Resources

Microsoft Global Security Strategy and Diplomacy
www.microsoft.com/gssd

Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust
aka.ms/supply-chain-risk

Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity
aka.ms/Trusted-Supply-Chain

The Microsoft Security Development Lifecycle
www.microsoft.com/sdl

The Software Assurance Forum for Excellence in Code (SAFECode)
www.safecode.org