Subject:- **Advisory - Prevention against Supply Chain Attack (Advisory No. 34)**

1. **Context.** In the wake of Sunburst malware attack (December 2020), prevention of supply chain attacks has become pivotal for sensitive organizations. Such attacks occur when a cyber-threat actor infiltrates a software vendor's network and injects malicious code in the software prior to its distribution to the customers. The infected software eventually compromises the customer's data / system. Due to **complexity** of **detection** and **trusted nature** of **vendor's software,** it becomes difficult to determine the **software supply chain attack.** Therefore, **recommendations** at **Para 4** may be followed to prevent software supply chain attacks.

2. **Techniques - Software Supply Chain Attack**

   a. **Hijacking Updates.** Software vendors typically **distribute updates** to customers from **centralized servers** as a routine part of product maintenance. Threat actors can **hijack** an update by **infiltrating** the **vendor's network** followed by either injecting **malware** into the **outgoing update** or altering the update to **grant** the threat actor **control** over the software's functionality.

   b. **Undermining Code Signing.** Code Signing is used to **validate** the **identity / integrity** of the code's author. In such cases, attackers undermine code signing by **self-signing certificates, breaking signing systems** or **exploiting misconfigured** account access controls. By undermining code signing, threat actors are able to successfully hijack software updates by impersonating a trusted vendor and inserting malicious code.

   c. **Compromising Open-Source Code.** **Open-Source Code** compromises occur when threat actors insert **malicious code** into **publicly accessible libraries,** which are afterward used by ordinary developers in their own code without knowing its harmful consequences.

3. **Consequences of Software Supply Chain Attacks.** The consequences of Software Supply Chain attack can be severe such as: -

   a. Threat actors use the **compromised software Vendor to· Gain privileged** and **persistent access** to a victim's network.

   b. By compromising a software vendor, the attackers **bypass perimeter security measures** like borders routers, firewalls etc and gain initial access.

   c. If threat actors loses network access, they may **re-enter** a network using the **compromised software vendor.**

   d. As a follow on action, threat actor may **inject additional tailored malware packages** into a **chosen target.**

   e. The additional malware may allow threat actor to conduct various malicious

activities that may include performing **data** or **financial** theft, **monitoring individuals** or **organization** and **disabling** networks or systems.

4. **Recommendations**

a. **Actions by Customer / Organizations.** Organizations acquiring software should consider its use in the context of a risk management program; **Cyber Supply Chain Risk Management (C-SCRM).** In addition, following best practices may be opted: -

1. Integrate C-SCRM across the organization and establish a formal C-SCRM program: -
    a. Identify **key mission** or business processes; what essential services does the organization provide.
    b. Maintain an **inventory of own organization's current** and **future software licenses.**
    c. Research and document how each **software license** is **supported** by its **suppliers;** are **patches** provided? Does the **supplier offer periodic email updates** about the product?
    d. Understand how your **organization's software supports** or is related to **organization's key processes?**
    e. **Document** to **address software** for which a **vulnerability** is disclosed.
2. Know and manage **critical components** and **suppliers.**
3. Understand the **organization's supply chain.**
4. Closely collaborate with key suppliers.
5. Include **key, suppliers** in **resilience** and **improvement** activities.
6. **Asses** and **monitor** throughout the supplier relationship.
7. Organization/ customer should request a **software component inventory** with each contemplated software purchase.
8. If a vendor cannot provide a **component inventory** of its software / hardware, consider using that as a differentiator when selecting among competing products.

b. **Actions by Software Vendor.** Software vendor must implement and follow a **software development life cycle (SDLC)** in course of software supply. The vendor must prepare **secure software development.** Guidelines are as under: -

1. Defining **software development security requirements.**

2. Establish **Secure Software Development Framework (SSDF)** roles and responsibilities within the SDLC.

3. Automating **developer, security toolchain** and establishing **software security criteria** and process to collect the data necessary for security checks.

4 **Software Operational Aspects**

a. Strict **application** and **IP whitelisting** of vendor's software should be performed. Vendor must provide list of **IPs and URLs** allowed to communicate with provided software and all other communication/ application access may be restricted / blocked.

b. Vendor should perform in-house and third-party code review, analysis, and testing before every release of software.

c. Vendors should provide a mechanism for **verifying software release integrity** (in particular, the protection of the code signing certificate) to help customers ensure that the software being acquired is not subjected to tampering.

d. Vendor should timely provide vulnerability information to organization point of contact as soon as the vulnerability information becomes available.

*****