BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 22-043 **April 2022, Issue #75**

BusinesSafe National Supply Chain Integrity Month

April is National Supply Chain Integrity month. This year, the theme is "Fortify The Chain," which is meant to encourage organizations to strengthen their information and communications technology (ICT) supply chain. The ICT supply chain is the network of retailers, distributors, and suppliers that operate in the creation, production, sale, delivery, of hardware, software, and managed services. The Cybersecurity and Infrastructure Security Agency (CISA) offers more information on the Fortify The Chain campaign on their website.

Threats and Vulnerabilities

The ICT supply chain for software and hardware faces many different threats, including cyber threats, which can affect manufacturers and users. ICT supply chain organizations and government agencies actively work to identify, mitigate and ensure resiliency against these threats. However, cybercriminals may still target the ICT supply chain and exploit vulnerabilities in an effort to compromise organizations that rely on widely-used hardware, devices, or software. Cyber threat actors may use a variety of methods to compromise systems including hijacking updates, network intrusions, code compromising, data exfiltration, and other attack types. This article touches on a few of the most common types of threats the ICT supply chain faces but is not all-encompassing.

1. **Cyber –** A software supply chain attack occurs when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or system. To address these threats, organizations can work closely with service providers to mitigate against these threats and implement or exercise a resiliency plan in place in the event of a cyber incident.
   Alleged hacker behind Kaseya ransomware attack extradited, arraigned in Texas
   Russians Tied To The SolarWinds Cyberattack Hacked Federal Prosecutors, DOJ Says

2. **Insider threat or data theft –** Cybercriminals may use trusted insiders or cyber attacks to disrupt or exfiltrate data to commit industrial espionage or steal intellectual property or personal identifiable information. Some cyber criminals may try to sell the data on the dark web or hold it for ransom. In some instances, data may also be stolen by a foreign government or cybercriminals working on their behalf.
   Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology
   Microsoft confirms breach, attributes attack to Lapsus$

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN:1.1, 1.10 FFC: 1, 6

3. **Outdated and unpatched systems -** Using outdated or unpatched software or devices creates vulnerabilities that can be exploited by cybercriminals to gain access to a network or launch an attack. It's important for organizations to install patches and updates as soon as they become available. Additionally, current shortages of semiconductors may increase production time for electronic devices and hardware, so organizations may want to factor additional time into planning for replacement of hardware and devices approaching end-of-life.
   Semiconductor Supply Chain Resiliency
   Understanding Patches and Software Updates

References:

- CISA offers multiple resources including alerts about current issues, vulnerabilities, and exploits as well as steps organizations can take to protect themselves and mitigate against these threats.
- The Office of the Director of National Intelligence website offers information and resources for ICT organizations as well as other critical infrastructure sectors for protecting their supply chains.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN:1.1, 1.10 FFC: 1, 6