BUSINESSAFE

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 23-057 **May 2023, Issue #102**

BusinesSafe Highlight – Supply Chain Resiliency

Supply chains are comprised of a series of processes that contribute to the production of goods and services for consumers. In supply chains, raw materials are transformed by producers, manufacturers, vendors, transporters, distributors and retailers into final products and services. Supply chains face a number of risks due to their multilayered structure and vulnerabilities to disruption. One compromised link in a supply chain could have serious consequences for other components and the finished product. Malicious actors can cause disruptions, whether physical or intellectual, and cause major supply shortages. Although the supply chain is vulnerable to a plethora of disruptions, the potential impacts due to cyber-attacks remain a constant focus.

How to Protect Your Business

1. Third-party risk assessments will help discover supply chain security risks before criminals exploit them. Each assessment should be customizable to accommodate each supplier's unique risk profile. Completing a customizable risk assessment could prove helpful.
2. To decrease the amount of data compromised due to a security breach, encryption practices should be placed on all forms of data. As an aid, the Advanced Encryption Standard should be implemented to protect electronic data.
3. Incident response planning is vital to preparation for every supply chain attack scenario. In the event of an attack, an appropriate response should be planned, coordinated, and strategic. Incident responses help organizations minimize loss, patch exploited vulnerabilities, restore affected systems and processes, and close the vector that was attacked.
4. Companies and organizations should do the following: 1) Review open source information regarding a partner's history of intellectual property theft. 2) Identify what was compromised, stolen, or attacked, and if possible, by whom. 3) Afterwards, consider the potential impact of your own security.
5. If operating within a government agency, review the Federal Bureau of Investigation's (FBI) supply chain risk management (SCRM).

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL 8888, Approval: FL 8900, HSEC:1. 6 FSIN: 1.5.1 FFC: 1.1, 1.2, 1.5, 4.4, 6.5, 6.9

How to Report

- In the event of an emergency, dial 911.
- "If You See Something, Say Something" - Report suspicious activity to your local law enforcement agency, on the FDLE website using Florida's “See Something, Say Something” Tool Kit or by calling 1-855-FLA-SAFE.
- Report computer security incidents to CISA’s Incident Reporting System.
- File a complaint with the Federal Bureau of Investigation’s Internet Crime Complaint Center (IC3).
- Report a computer crime and security incident to the Florida Department of Law Enforcement (FDLE).

Resources

- Cyber Security and Infrastructure Security Agency (CISA) offers a comprehensive resource for supply chain integrity.
- The Office of the Director of National Intelligence (ODNI) provides an overview of tactics used in software supply chain attacks.
- The Federal Bureau of Investigation (FBI) describes recommended practices for developing a supply chain risk assessment.
- The National Institute of Standards and Technology (NIST) offers ample information on software security in supply chains.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL 8888, Approval: FL 8900, HSEC:1. 6 FSIN: 1.5.1 FFC: 1.1, 1.2, 1.5, 4.4, 6.5, 6.9