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 19-281 **December 2019, Issue #15**

BusinesSafe Threat Topic: Cyber Supply Chain Risks

Supply chains are comprised of a series of processes that contribute to the production of a good or service for consumers. In supply chains, raw materials are transformed in a series of steps into a final product or service through work done by producers, manufacturers, vendors, transporters, distributors, and retailers. Supply chains face a number of risks due to their multi-layered structure and can be vulnerable to disruption. One compromised link in a supply chain could have serious consequences for other components and the finished product.

Supply chains can be compromised in a number of ways, including via technological components. An entity's cyber components can be compromised if, for example, spyware is installed on a computer's hard drive by a supplier or criminal actors before it is shipped to a company. Any information that the user inputs on the device can now be accessed by the supplier. In other instances, a threat actor can gain access to a company by compromising a service provider whose product has access to the target company's network or servers.

Recent Incidents

In 2019, job recruitment website, Monster, reported that a third-party vendor left a web server exposed containing thousands of resumes for users between 2014 and 2017. These documents contained sensitive information including names, phone numbers, addresses, and in some instances, immigration documents.
Job Recruitment Site, Monster.com Suffers Data Breach

In 2019, LabCorp and Quest Diagnostics reported an unauthorized intrusion that impacted over 12 million customers. The data breach exposed credit card, banking, and medical information as well as personally identifiable information for eight months. The breach was caused by an initial intrusion into the networks of the companies' billing collections service provider.
Checking for Vitals: Inside the Quest Diagnostics, LabCorp Supply Chain Breach

In 2013, a Target store's computer systems experienced a data breach that caused the compromise of roughly 110 million individuals' credit and debit card information. In this instance, the weak link in this supply chain was a refrigeration contractor. This third-party entity received

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1

at least one phishing email which, when activated, was able to install malware onto their computers and grant access to secure information used to infiltrate Target's networks.
Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned

Ways to Manage Cyber Supply Chain Risks

1. Identify vulnerabilities within your supply chain and develop countermeasures to address these.
2. Carefully vet potential industry partners (vendors, manufacturers, distributors, etc.) and remain attentive to changes in partner ownership.
3. Limit the number of individuals with access to critical systems and only give them access to what they need to complete their task.
4. Regularly inspect equipment, hardware, and software for tampering.
5. Ensure software and antivirus protection is updated and install patches in a timely manner.
6. Train personnel to understand threats and risks within a supply chain as well as how to recognize and report suspicious activities.

Resources
The following document provides an overview of tactics used in software supply chain attacks.
ODNI: Software Supply Chain Attacks

The following document lists helpful steps in developing a supply chain risk management program (SCRM).
ODNI: Baker's Dozen -13 Elements of an Effective SCRM Program

The following link describes recommended best practices for developing a supply chain risk assessment and neutralizing risks.
FBI: Best Practices in Supply Chain Risk Management for the U.S. Government

To sign up to receive BusinesSafe directly to your email, visit our website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1