CTPAT ALERT

Cyber Threats – The Cloud and Remote Connections

Last Updated: January 22, 2021

To enhance communication with its Members, the Customs Trade Partnership Against Terrorism (CTPAT) program routinely highlights security matters for the purpose of raising awareness and renewing Partners' vigilance in supply chain security. This CTPAT Alert highlights threats posed to Members that utilize cloud-computing solutions and/or have employees working remotely.

In response to the COVID-19 pandemic, many Members transitioned a portion of their workforce to remote computing, or teleworking. Recent, open-source reporting, suggests that many companies may allow employees to work remotely on a permanent basis even after the threat from COVID-19 subsides.

Since the onset of the pandemic, threat actors have attempted to exploit weaknesses associated with remote computing configurations and have targeted employees directly through email phishing attacks (and via phone) to effect a number of adverse actions. It has historically been a common tactic of hackers to exploit disasters, pandemics and major political events to launch targeted and convincing phishing campaigns. Globally, businesses have reported an increase in unauthorized network intrusions, loss of data, and holding data for ransom.

Businesses can elect to conduct only a portion of, or most of their business processes using cloud-based solutions. Cloud services can include, but are not limited to truck dispatching, enterprise resource planning (ERP), file storage, and enterprise email. Some CTPAT Members have stated that since most of their business transactions are carried out in cloud-based solutions, that they are not required to follow or implement some or all of the cybersecurity minimum-security-criteria (MSC). This could not be farther from the truth. Operating in the cloud, to any degree, does not alleviate a CTPAT Member's responsibility to adhere to the MSC and follow practical and reasonable cyber security practices.

Earlier this month, the Cybersecurity and Infrastructure Security Agency (CISA), a component agency of U.S. Department of Homeland Security (DHS), issued *Analysis Report AR21-013A: Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services.* According to this report, "threat actors are using phishing and other vectors to exploit poor cyber hygiene practices within a victims' cloud services configuration". In other words, CISA contends that companies that operate in a cloud environment are still very much at risk from the threats posed by cyber threat actors.

For example, CISA has observed cyber threat actors using phishing emails with malicious links to harvest credentials (meaning hackers send phishing emails with harmful links and use sophisticated tools to extract/steal username/password combinations) from users' cloud service accounts. Cyber criminals include a link on those phishing emails to make them appear as secure messages or emails coming from a legitimate file hosting service account login – please see link to FBI announcement on spoofing at the end of this alert.

CTPAT ALERT

Cyber Threats – The Cloud and Remote Connections

Last Updated: January 22, 2021

All CTPAT Members should ensure their employees are adequately trained on phishing campaigns and threats associated with web domain (web address) spoofing.

- CTPAT Points of Contact (POC) should discuss this CTPAT Alert and the CISA report with their IT personnel (https://us-cert.cisa.gov/ncas/analysis-reports/ar21-013a). The CTPAT cyber MSC should be reviewed to determine if, based on this information, there are weaknesses associated with remote connectivity solutions. This alert involves several of the CTPAT cyber security criteria.

- The CISA report outlines several actions that organizations can take to mitigate the threats and "…strengthen their cloud environment configurations to protect against, detect, and respond to potential attacks." Below are some of the most critical recommendations from CISA along with its corresponding CTPAT minimum-security criteria ID number.

  - ✓ Enforce multi-factor authorization (MFA) /Implement MFA for all users, without exception. Users should be required to have at least a second factor in order to enter a company's network - in addition to just a password or passphrase – MSC 4.8.

  - ✓ Consider a policy that does not allow employees to use personal devices for work. At a minimum, use a trusted mobile device management solution – MSC 4.10.

  - ✓ Consider restricting users from forwarding emails to accounts outside of your domain. While this is not always possible, consider adding a header to all outside emails that makes it clear they came from outside the company network. This should also be taken to mean that employees should be prohibited from sending email from the company network to their own, personal email address, and vice-versa. Also, consider prohibiting employees from accessing their personal, web-based email from company devices. – MSC 4.1 & 4.5.

  - ✓ Allow users to consent only to app integrations that have been pre-approved by an administrator. Restrict employees from downloading unauthorized programs, apps, etc. or making changes to or connections from one application to another without requisite approvals. This also includes turning off or making changes to antivirus software that is installed on their devices – MSC 4.1 & 4.5.

  - ✓ Focus on awareness and training. Make employees aware of the threats-such as phishing scams-and how they are delivered. Training is typically at the top of most cyber 'to-do' lists and is considered crucial. Many Members test their employees by sending harmless phishing emails to employees periodically – MSC 12.1 & 12.8

- ✓ Establish blame-free employee reporting to ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be deployed quickly and efficiently. Employees often see their antivirus program on their computer and believe the presence of that software, coupled with their IT department should be enough to keep their computer and network safe. This is not always the case. Employees should be encouraged to report possible suspicious activity – MSC 12.10.

Other Cyber Security Links

FBI – Spoofing of website addresses – Note: This Public Service Announcement was published in advance of the recent elections but the document is still relevant today. This link will open a pdf attachment.

Stop. Think. Connect. – The STOP.THINK.CONNECT.™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

CTPAT Cyber MSC Videos (YouTube) – CTPAT PowerPoint presentation training videos that specifically address how Members can meet key cyber security criteria.

CTPAT Program

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW Washington, DC 20229