CISA Community Bulletin - January 26, 2021

CISA Launches New Ransomware Campaign

Ransomware is a constantly evolving and increasing threat to both public and private networks. To help defend against and respond to ransomware attacks, the Cybersecurity and Infrastructure Security Agency (CISA) has launched its *Reduce the Risk of Ransomware Campaign*.

The campaign is a focused and sustained effort designed to raise awareness of important behaviors and actions about how organizations can help prevent ransomware attacks, protect organizational data in case it gets compromised, and properly respond to an attack.

The campaign provides public and private sector organizations with the necessary information, tools, and resources, including incident response services and network assessment capabilities, that are needed to help lessen the risks and threats from ransomware.

Explore the New Ransomware Webpage and Guide

As part of the *Reduce the Risk of Ransomware Campaign*, CISA also recently unveiled its new ransomware webpage, which includes links to no-cost tools available for organizations and individuals, as well as targeted resources for the K-12 community.

The webpage also includes CISA's recently-published ransomware guide which is released in partnership with the Multi-State Information Sharing and Analysis Center (MS-ISAC). The guide is a comprehensive, customer-centered resource featuring best practices and ways to prevent, protect, detect, and respond to ransomware attacks.

Learn More About Ransomware

Alerts and Announcements

CISA Releases New Courses on Cloud Security and Cybersecurity Foundations for Federal, SLTT, and Veteran Users

CISA is excited to announce two new Federal Virtual Training Environment (FedVTE) cybersecurity courses available to the public: Cloud Security and Foundations of Cybersecurity for Management. Federal, State, local, tribal, and territorial (SLTT) government, and Veteran users can also access these courses, track their progress, and store course transcripts.

- The two-and-a-half-hour Cloud Computing Security course will explore guidance from the Cloud Security Alliance, National Institute of Standards and Technology, National Security Agency, and several Cloud Service Providers. Topics will cover cloud security risks and threats, basic operations, incident response considerations, as well as application, data, and infrastructure security concepts.

- The two-hour Foundations of Cybersecurity for Managers course is for stakeholders involved in decision making for security in a cyber environment who do not have a strong technical background. The course will focus on cybersecurity concepts and methodologies involved in building a resilient cyber enterprise.

Visit the FedVTE Public Courses page to learn more about publicly available courses. For new Federal, SLTT, and Veteran users interested in creating an account, go to fedvte.usalearning.gov to sign up today.

If you have questions about courses or the FedVTE platform, please contact Sarah Johnson (Sarah.Johnson@cisa.dhs.gov) and Susan Hansche (Susan.hansche@cisa.dhs.gov).

CISA Identifies Data-Driven Security Best Practices for K-12 Schools in Simulation Experiment

CISA has released a report from a School Security Simulation Experiment (SIMEX) focused on security procedures and technologies to improve both physical and operational security in K-12 schools. The SIMEX, conducted jointly with MITRE and George Mason University in August, served as a pilot to determine whether a SIMEX is a viable tool that can be used to evaluate policies, technologies, and procedures related to school safety in the future.

“SIMEX represents the continuation of our work to protect schools with evidence-based strategies, resources, and best practices,” said CISA Acting Assistant Director for Infrastructure Security Scott Breor. “CISA will continue to work in partnership with Federal partners, states, districts, and communities to make our Nation’s schools more safe and resilient.”

The SIMEX was designed to develop recommendations for school administrators to enhance the security of their facilities and operations. High-level takeaways from this SIMEX included:

- In this experiment, it was found that the presence of a School Resource Officer increased the number of students reported safe within a classroom or outside the school and decreased the number of causalities during an active shooter incident in school.

- In this experiment, it was found that classroom doors that lock automatically when closed increased the number of classrooms that successfully completed lockdown procedures and increased the number of students reported safe during an active shooter incident in school.

The full results of this SIMEX have been documented in a formal After-Action Report, which is available on CISA's School Safety and Security web page.

CISA Solicits Public Comment: Advance Notice of Proposed Rulemaking on the Removal of Certain Explosive Chemicals from the Chemical Facility Anti-Terrorism Standards (CFATS)

For more than a decade, the CFATS program has made the Nation and its communities safer and more secure by requiring high-risk chemical facilities to implement security measures that reduce the risk of hazardous chemicals being weaponized by terrorists.

In July 2020, Congress reauthorized the CFATS Program for three years, providing much-needed stability not only for the regulated community, but also for CISA which manages the CFATS program. CISA continues to examine ways to streamline and enhance this program while ensuring that America's critical infrastructure remains secure.

CISA is soliciting public comment on an advance notice of proposed rulemaking (ANPRM) that considers removing 49 explosive chemicals from the list of regulated chemicals of interest in Appendix A of the CFATS regulation. These 49 chemicals are known as Class 1, Division 1.1 explosives and are subject to security regulations implemented by the Bureau of Alcohol, Tobacco, Firearms and Explosives.

An ANPRM is the first stage in the rulemaking process and is designed to garner public input and stakeholder feedback, which is critical to ensuring the CFATS regulation properly balances costs of implementation with security value. No regulatory changes are going into effect at this time.

CISA welcomes all input on this topic. The ANPRM on the Removal of Certain Explosive Chemicals from the Chemical Facility Anti-Terrorism Standards is open for comment for 60 days to March 8, 2021.

Events

Partner Webinar: Privacy in an Era of Change

Join the National Cyber Security Alliance and LinkedIn for Data Privacy Day 2021! This free event will will convene data privacy experts from industry, government, academia and non-profit for an afternoon of discussions on current topics in data privacy.

Date: January 28, 2021

Time: 12:00 p.m. ET

Partner Webinar: What You Need to Know About Cyber Insurance

Join the Cyber Readiness Institute (CRI) and CRI Champion Transmosis for a roundtable discussion aimed at helping small and medium-sized enterprises understand how cyber insurance works and what it covers.

Date: February 4, 2021

Time: 12:00 p.m. ET

Register Here

Partner Webinar: Small Business, Big Threat

The U.S. Small Business Administration is hosting a workshop to discuss the realities of cyber risk and the need for cyber security. Join this webinar to explore basic best practices and review scenarios and examples to help you protect you and your business.

Date: February 4, 2021

Time: 10:00-11:30 a.m. ET

Register Here

Featured Programs and Resources

New Bulletin Offers Insights on Major Bomb Attack in Nashville

In the aftermath of the Christmas Day bombing in Nashville, CISA has worked closely with the FBI National Explosives Task Force and law enforcement partners on security issues and sharing key resources.

Among these critical products is CISA's TRIP*wire* Awareness Bulletin, *December 2020 Nashville VBIED Attack: Incident Snapshot and Security Considerations*.

This bulletin provides key insights about the Nashville vehicle borne improvised explosive device (VBIED) explosion to Federal, SLTT, and private sector partners.

To read the full report, visit the TRIP*wire* Library's Awareness Bulletins. First time visitors will need to create an authenticated TRIPwire account.

CISA Releases Infographic Illustrating Physical Security Measures for COVID-19 Vaccine Distribution

CISA is pleased to announce the release of the *COVID 19 Vaccine Distribution Physical Security Measures Infographic*, which illustrates four stages of vaccination distribution activity, possible physical threats at these stages, and proposed corresponding mitigation methods.

The infographic identifies manufacturing centers, transporters, clinics, pharmacies, and healthcare facilities, and points of distribution.

To learn more about CISA information and updates on COVID 19, visit the CISA Coronavirus page or download the infographic from the CISA Publications Library.

CISA Rolls Out New 5G Resources

CISA published a Critical Infrastructure Security and Resilience Note, *Edge vs. Core An Increasingly Less Pronounced Distinction in 5G Networks*, to inform stakeholders about the risks of untrusted components within 5G networks.

This product is intended to provide an overview of edge computing and represents CISA's analysis of the risks associated with installation of untrusted components into 5G infrastructure.

CISA also released its 5G Strategy and 5G Basics Infographic to educate stakeholders on key challenges and risks associated with the technology underpinning 5G networks.

To learn more about CISA's role in 5G, visit CISA's 5G site.

Supply Chain Lessons Learned During COVID-19

CISA has published an analysis report, *Building A More Resilient ICT Supply Chain: Lessons Learned During The COVID 19 Pandemic*, examining how information and communication technology (ICT) supply chain logistics have been impacted by the COVID 19 pandemic. Developed by industry members of the ICT Supply Chain Risk Management (SCRM) Task Force, the report provides practical recommendations to increase supply chain resilience against future risks.

The Task Force formed a COVID 19 Impact Study Working Group, which studied how key supply chain operational areas such as inventory management, supply chain

mapping/transparency, and supply chain diversity were impacted by the shocks of the pandemic. The Working Group identified three major stress points:

1. The unpreparedness of some manufacturing companies because of their reliance on lean inventory models (e.g., inventory shortages).

2. The difficulties companies faced in understanding who their junior tier suppliers were and where they were located (in case junior tier supplies experienced interruptions, shutdowns, etc.).

3. The need for a different approach diversifying supply chains to a broader array of locations instead of from single source/single region suppliers.

In the face of today's realities, private public coordination is essential to enhance ICT supply chain resilience to protect against tomorrow's threats.

For more information and resources about ICT supply chain, and to read the report, visit cisa.gov/ict scrm task force.

Download the COVID-19 Impact Study

CISA Publishes *Cybersecurity and Physical Security Convergence Action Guide*

CISA is excited to announce the publication of the *Cybersecurity and Physical Security Convergence Action Guide*, which provides guidance on converging cybersecurity and physical security functions to better position organizations to mitigate cyber physical threats.

The action guide provides information on convergence and the benefits of a holistic security approach that aligns cybersecurity and physical security functions with organizational priorities and the cyber physical threat landscape. In addition, the guide describes the complex operating environment, the risks associated with siloed security functions, convergence in the context of organizational security functions, and provides a flexible framework for aligning security functions.

For more information or to access the guide, visit the CISA Publications page.

CISA Releases Tribal Emergency Communications Resources

CISA has released two new pieces of information to support communications infrastructure for Native American and Alaska Native Tribes in the interests of public safety and human services:

- The *CISA Tribal Emergency Communications Program Brochure* provides an overview of all tribal communications governance and technical support services offered by CISA.

- The *CISA Tribal Emergency Communications Resources Fact Sheet* provides a list of key resources and resource libraries of interest to tribes seeking support by way of governance and planning, technical assistance, funding, and priority services.

These materials can be downloaded from the CISA publications webpage. For more information, please contact cisatribalaffairs@cisa.dhs.gov.

Learn More About Emergency Communications Here

CISA Releases New Security Resources for Faith-Based Communities

CISA is committed to supporting efforts to maintain safe and secure houses of worship and related facilities while sustaining an open and welcoming environment.

Last month, CISA released the *Power of Hello Guide for Houses of Worship* and the *Mitigating Attacks on Houses of Worship Security Guide* to provide insightful information and analysis pertaining to recognition, prevention, and intervention strategies that can be taken to mitigate risk from an attack.

- The *Power of Hello Guide for Houses of Worship* was developed specifically for the faith based community and assists in identifying and properly responding to suspicious behavior. The document guides houses of worship and related facilities with identifying questions that can be asked when navigating a potential threat, know when and how to obtain help, and outlines incident response best practices.

- The *Mitigating Attacks on Houses of Worship Security Guide* is a comprehensive security guide that assesses potential threats posed to the faith based community based on an analysis of 37 incidents that occurred in the U.S. from 2009 2019 and corresponding tangible actions / protective measures that the community can leverage to mitigate risk.

To view additional faith based resources, visit CISA's Faith Based Community Resources page.

For more information on the DHS Active Shooter Program, please visit CISA's Active Shooter Preparedness page.

Social Media

Help CISA spread the word about upcoming events and new resources by sharing the following posts via your social media channels. Thank you for your support!

- Have you heard? @CISAgov just launched a new #ransomware campaign! For more information, visit CISA.gov/ransomware and continue to #BeCyberSmart about your cybersecurity!

- #Ransomware attacks increased during the #COVID19 outbreak. @CISAgov offers advice on protecting you and your organization: CISA.gov/ransomware

- The #supplychain gets our food and medicine to us safely. Read how @CISAgov studied the effects of #COVID-19 on the ICT supply chain: cisa.gov/ict-scrm-task-force