CISA Community Bulletin - May 26, 2021

CISA Releases Best Practices for Preventing Business Disruption from Ransomware Attacks

In light of the recent ransomware attack on the Colonial Pipeline, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) urge critical infrastructure (CI) asset owners and operators to adopt a heightened state of awareness, as well as implement the recommendations listed in the Mitigations section of this Joint Cybersecurity Advisory.

Some of these recommendations include:

- Filtering network traffic to prohibit ingress and egress communications with known malicious IP addresses;
- Enabling strong spam filters to prevent phishing emails from reaching end users;
- Implementing robust network segmentation between information technology and operational technology networks; and
- Regularly testing manual controls; and ensuring that backups are implemented, regularly tested, and isolated from network connections.

These mitigations will help CI owners and operators improve their entity's functional resilience by reducing their vulnerability to ransomware and the risk of severe business degradation if impacted by ransomware.

Learn More About Preventing Business Disruption Here

Alerts & Announcements

CISA and NFL Host Webinar on Priority Telecommunications Services

CISA and the National Football League (NFL) partnered to present a webinar entitled, “Jump to the Head of the Line! Priority Services for Emergency Communications” in support of Implementing the National Emergency Communications Plan (NECP).

The webinar discussed adoption and use of CISA’s Priority Telecommunications Services (PTS) and shared solutions offered in the NECP to ensure continuity of communications.

During an emergency, it is crucial that emergency responders can communicate. However, potential congestion and the inability for responders to successfully complete calls is a threat. PTS allows prioritized access to wireless communications networks for qualified, pre-registered users, providing them the ability to “cut the line” and complete their mission-critical communications.

During the webinar, panelists discussed the services and key features of PTS, as well as the NFL’s subscription to priority services for its Global Security Operations Center. Eventually, PTS protocols will be incorporated into all of the NFL’s business and game-day standard operating procedures.

To receive a copy of the webinar slide deck, which includes a comprehensive list of resources, please send a request to necp@cisa.dhs.gov.

Executive Order on Improving the Nation's Cybersecurity

On May 12, President Biden signed the *Executive Order on Improving the Nation’s Cybersecurity* to support the nation’s cybersecurity and protect the critical infrastructure and federal government networks underlying the nation’s economy and way of life.

“President Biden’s executive order is an important step forward in bolstering our nation’s cybersecurity." said CISA Acting Director Brandon Wales. "As last week’s ransomware attack against the Colonial Pipeline and recent intrusions impacting federal agencies demonstrate, our nation faces constant cyber threats from nation states and criminal groups alike."

CISA will support a number of cybersecurity efforts through the Executive Order, including:

- Developing a federal cloud security strategy and a cloud service governance framework;
- Refining the process for coordination and collaboration on cybersecurity and incident response for cloud technology to foster better understanding of roles and responsibilities as well as visibility;
- Driving adoption of multifactor authentication and encryption for data at-rest and in-transit within six months;

- Working with the National Institute of Standards and Technology (NIST) as they develop an initial list of secure software development lifecycle standards for software purchased by the Federal Government and minimum testing requirements for software source code; and
- Working with the General Services Administration (GSA) and the Office of Management and Budget (OMB) to modernize the Federal Risk and Authorization Management Program (FedRAMP) to help agencies implement a standardized approach to cybersecurity that takes into account the rapidly changing threat landscape and facilitates agility in solution adoption.

Visit the CISA website for more resources, including links to the White House Fact Sheet and the full Executive Order.

Learn More About Executive Order 14208 Here

CISA Protects Critical Infrastructure Information Through PCII Program

CISA's Protected Critical Infrastructure Information (PCII) Program protects private sector and state, local, tribal, and territorial (SLTT) infrastructure information voluntarily shared with the government for the purposes of homeland security from disclosure under the Freedom of Information Act, state and local disclosure laws, civil action and regulatory proceedings.

Despite the challenges of the COVID-19 pandemic, CISA’s PCII Program Office not only continued operations with stakeholders, but also increased its tempo through remote work, thus proving its flexibility to support major events such as the 2020 election and the NFL’s Super Bowl.

Since 2004, the PCII Program Office has validated and protected over 127,000 submissions. with over 4,400-plus PCII Authorized Users accessing the information on a need-to-know basis, the flexibilities built into information collection, protection, and sharing ensure the PCII Program is a value-added tool for stakeholders.

Learn More About the PCII Program Here

CISA Releases 2020 Year in Review

Early in 2020, COVID-19 emerged as a top priority for CISA and the nation. As the pandemic spread across the United States, nearly all CISA’s employees transitioned to full time telework starting March 13, 2020, and retained mission continuity while maintaining the health and safety of employees and their families.

Despite an abrupt transition to a fully virtual environment, CISA continued to engage with stakeholders and partners around the nation and the world to understand and mitigate risks to the nation’s cyber, physical, and emergency communications infrastructure.

The 2020 Year in Review showcases key examples of CISA's work to carry out its mission in 2020, including milestones and accomplishments as the Agency advanced strategic priorities to maintain a secure and resilient infrastructure for the nation.

Learn More About the Year in Review Here

Events

Webinar: Leveraging the Whole Community to Make Critical Emergency Communications Decisions

This National Emergency Communications Plan webinar will feature representatives who are actively building more inclusive emergency communications governance bodies.

Date: May 26, 2021

Time: 1:00 p.m. EST

Learn More Here

Partner Webinar: Defending Your Small Business From Big Threats

Join the National Cyber Security Alliance for a *CyberSecure My Business* webinar to learn how to defend small businesses from present-day cyber threats.

Date: June 1, 2021

Time: 2:00 p.m. ET

Learn More Here

Virtual Seminar: EMP & GMD Grid Resilience Seminar

CISA is co-hosting a seminar for government and industry leaders and experts on how to enhance the security and resilience of the nation's electric grid from electromagnetic pulse (EMP) attacks or a naturally occurring geomagnetic disturbance (GMD).

Date: June 8, 2021

Time: 1:00 p.m. ET

Learn More Here

Featured Programs and Resources

The ICT Supply Chain Risk Management Task Force Releases New Resources

CISA, other federal agencies, and representatives from information and communications technology (ICT) private sector companies and associations formed the ICT Supply Chain

Risk Management (SCRM) Task Force to develop strategies to mitigate and address supply chain risks faced by industry.

With over 70 industry representatives, the Task Force is the nation's leading public private supply chain risk management endeavor that has worked together to develop a number of products that incorporate industry standards to help organizations increase their resilience.

The ICT SCRM Task Force is pleased to share new resources that can assist organizations and businesses assess the trustworthiness of their vendors and suppliers:

- **ICT Supply Chain Risk Management Toolkit**: This Toolkit which includes strategic messaging, social media, videos, and resources is designed to emphasize the role that we all have in securing ICT supply chains. All the products incorporate industry standards to make them highly effective tools to help increase supply chain resilience. Stakeholders can use this Toolkit to inform their personnel, vendors, suppliers, partners, and others about their role in supply chain risk management and help spread awareness of this important effort.

- **Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists**: This report provides organizations a list of criteria and factors that can be used to inform an organization's decision to build or rely on a qualified list for the acquisition of ICT products and services.

- **Vendor SCRM Template**: This template provides a set of questions regarding an ICT supplier/provider's implementation and application of industry standards and best practices. The results can be used to help guide supply chain risk planning in a standardized way and provide clarity for reporting and vetting processes when purchasing ICT hardware, software, and services.

Learn More About the ICT SCRM Task Force Here

CISA Releases New Web Page on Securing Public Gatherings

Last month, CISA announced the launch of the CISA Securing Public Gatherings web page. Public gatherings and crowded places are increasingly vulnerable to terrorist attacks and other extremist actors because of their relative accessibility and large number of potential targets.

The new CISA Securing Public Gatherings web page provides resources to help secure public gatherings in an open and welcoming environment, as well as helping address threats impacting:

- Businesses and critical infrastructure owners and operators,
- State, local, tribal, and territorial (SLTT) government officials and first responders,
- Houses of worship,

- Schools; and
- The general public.

Explore the new web page to find resources to help organizations mitigate potential risks in today's dynamic and rapidly evolving threat environment.

Learn More About Securing Public Gatherings Here

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!

- Check out this new graphic novel from @CISAgov on combating disinformation https://www.cisa.gov/news/2021/04/28/cisa-releases-second-graphic-novel-combat-disinformation-national-superhero-day
- Want to learn more about securing 5G infrastructure from cybersecurity risks? @CISAgov has the resources you need www.cisa.gov/5G
- Crowded gatherings are increasingly vulnerable to terrorist attacks. @CISAgov just launched web page to secure public gatherings https://www.cisa.gov/securing-public-gatherings