Office of the
Chief Information Security Officer
State of Texas

Cybersecurity Activity and Considerations Bulletin

TLP:WHITE

June 16, 2022

The Texas Department of Information Resources (DIR), in coordination with the Texas Information Sharing and Analysis Organization (TX-ISAO), is issuing the June 2022 Cybersecurity Activity and Considerations Bulletin for awareness and consideration by all Texas government organizations.

Cybersecurity incidents can significantly disrupt the ability of government organizations to serve their constituents. This bulletin provides an overview of recently observed activity, suggested actions to increase resilience from attacks, and additional authoritative resources and guidance.

Considerations to Improve Security

There is no single tool, solution, or process that can eliminate the risk of ransomware attacks but adopting cybersecurity best practices and taking the proactive measures provided below can minimize an organization's risk of significant ransomware impacts.

BEST PRACTICES

- Develop a strong culture of cybersecurity awareness
- Create an incident response plan
- Establish a functional vulnerability and patch management program
- Maintain reliable backups
- Coordinate tabletop exercises with organization leadership and technical staff
- Implement multi-factor authentication (MFA)
- Deploy Endpoint Detection and Response (EDR) solutions

SHORT-TERM STEPS

Engage the TX-ISAO

The TX-ISAO serves as a central clearinghouse for cybersecurity intelligence. Members receive security bulletins on vulnerabilities, emerging threats, and other cyber activity.

Backup Systems and Data

Establish regular automated backups and redundancies of key systems. Employ a backup solution that automatically and continuously backs up business-critical data and system configurations. Make sure that all mission-critical data is enumerated. Test your backup strategy before using it.

Develop an Incident Contact List

Develop and print out a list of internal and external contacts in case of a cybersecurity incident. These may include your organization's leadership, law enforcement, DIR, and other response partners.

Report Suspicious Cyber Activity

Report suspicious or anomalous activity in IT systems to the TX-ISAO by submitting a threat report. A TX-ISAO partner will follow up and provide guidance or context to the observed activity. Urgent notifications of cyber incidents can be made to the DIR Security Incident Hotline at (877) 347-2476.

MEDIUM-TERM STEPS

Develop an Incident Response Plan

DIR's Incident Response Team Redbook provides a guide for organizations to use in developing an incident response plan. Coordinating the team, the activities, and methods for responding to a cybersecurity incident in advance of an attack will benefit an organization's response posture. Print out the response plan so it is available in case of a cybersecurity incident.

Inventory and Document IT Assets

Develop a network diagram and create a software and hardware inventory of your organization's IT environment. Print out the inventory and documentation so it is available in case of a cybersecurity incident.

Exercise Your Incident Response Plan

Conduct a tabletop (or discussion-based) exercise to work through the technical and non-technical response to a cybersecurity incident. Invite a diverse audience to these tabletops, including IT staff, executive management, communications, legal, human resources, elected officials, and other personnel identified in your organization's incident response plan.

Join MS-ISAC

Consider joining the Multi-State Information Sharing and Analysis Organization (MS-ISAC) and review the free and reduced-price services available to members. Free services include Malicious Domain Blocking and Reporting (MDBR) and incident response services, and reduced cost services include network monitoring and EDR solutions.

Onboard into DIR Managed Security Services

Organizations are encouraged to onboard into the DIR Managed Security Services (MSS) program and complete an Interlocal or Interagency Contract at no cost. In case of a cybersecurity incident where additional resources are needed, onboarded entities have quick access to security incident management services at a competitive rate without having to pay a traditional retainer.

Email dirsharedservices@dir.texas.gov to request a new customer form to start the onboarding process.

Vulnerability and Patch Management

Keeping IT systems up to date with the latest security patches will reduce the likelihood of cyber criminals exploiting known vulnerabilities in IT systems. The federal Cybersecurity and Infrastructure Security Agency (CISA) provides no-cost cyber hygiene scanning services and identifies vulnerabilities actively being exploited to help prioritize patching efforts.

LONG-TERM STEPS

Focus on Business Continuity and Disaster Recovery

Developing a business continuity and disaster recovery plan based on a comprehensive business impact analysis will provide a framework for recovery and the ability to conduct business if your organization is impacted by a ransomware attack or other cybersecurity incidents.

Consider Endpoint Protection

Evaluate an EDR solution within your environment and consider investing in EDR technology to improve endpoint visibility and to help mitigate cybersecurity threats.

Enable Multi-Factor Authentication

Logins protected with MFA are more secure because multiple verification methods are required to authenticate access into systems. Implementing an MFA solution increases the resilience of your organization. Additionally, credential monitoring activities may provide advanced insight into potentially compromised and privileged users.

Additional Resources and Guidance

CYBER INSURANCE

If your organization has a cyber insurance policy, it is important to know how to file a claim and to include relevant contact information in the incident contact list or incident response plan.

REFERENCE LINKS

Reducing the Significant Risk of Known Exploited Vulnerabilities

- Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Multi-State Information Sharing and Analysis Center (MS-ISAC)/ CISA Joint Ransomware Guide

- https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

TECHNICAL REFERENCES

FBI FLASH: BlackCat/ALPHV Ransomware Indicators of Compromise

- https://www.ic3.gov/Media/News/2022/220420.pdf

NIST SP: 800-209: Security Guidelines for Storage Infrastructure

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf