ENTERPRISE
information services

CYBER SECURITY SERVICES

RANSOMWARE AWARENESS CAMPAIGN

August 2023 | Volume 3

PROTECT

Protect

Protect is the second of five core functions within the Cybersecurity Framework (CSF). The function of protect is to limit or contain the impact of ransomware events. There are three categories within protect that we will cover.

Identity Management & Access Control – The purpose of Identity Management & Access Control is to limit who has access to information/systems and verify they are who they say they are. These include:

- Ensuring user accounts with administrator-level privileges are never used to browse the internet or access email. Employees should be directed to use a regular computer account for daily work.
- Ensuring unused or stale computer accounts are regularly reviewed and disabled or deleted.
- Requiring the use of long complex passwords/ passphrases with a regular password reset interval.
- Utilizing Multi-Factor Authentication (MFA) on cloud-based accounts, when possible.

Awareness & Training – Because most ransomware events start by exploiting an organization's users, security awareness training can be highly effective in mitigating potential ransomware events. These include:

- Phishing awareness training – Teach employees how to recognize suspicious emails and report them.
- Social engineering training – Train employees how to recognize attacks that try to trick them into sharing sensitive information by using manipulation, impersonation and persuasion.

GOAL: The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.

Cyber Security Services Webinar - Save the Date!

» October 11, 2023 1pm – 2pm
» October 13, 2023 9am – 10am

PROTECT IS ESSENTIAL FOR:

» Understanding the need for different technologies to help mitigate ransomware events
» Stopping ransomware from reaching your users
» Blocking harmful or malicious content before they reach your systems
» Limiting the effect and impact of ransomware events

For more information scan the QR code or visit our website
ransomwareinfo.oregon.gov

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

Protective Technology – Protective technology refers to a range of tools designed to enhance the safety of an organizations IT assets. This technology is intended to mitigate risks, prevent accidents, deter threats, and respond effectively to various types of dangers. These include:

- **Anti-Malware (Anti-virus) software** – Ensure it is being kept up-to-date. It is designed to detect, prevent, and remove malicious software, or "malware," from computers, networks, and devices. It plays a critical role in maintaining the security and integrity of digital systems by identifying and neutralizing various types of malware threats.
- **Anti-spam email communication protections** – Spam emails are unsolicited, often irrelevant, or inappropriate messages sent in bulk to a large number of recipients. These emails can range from annoying advertisements to phishing attempts, scams, and even malicious software distribution.
- **Internet content filtering** – Web content filtering or web filtering, refers to the process of controlling and managing the types of online content that users can access while browsing the internet. It can help by preventing users from accessing websites that contain inappropriate, offensive, or explicit content, which often contain malicious code.
- **Domain Name Service (DNS) filtering** – A technology that is used to control and manage access to websites and online content based on domain names. It can help protect the organization in the event an employee clicks on a malicious email link.
- **Software patching and vulnerability management** – Software patching and vulnerability management plays a crucial role in mitigating the impact of ransomware attacks by addressing vulnerabilities in software and operating systems that attackers often exploit. Ransomware attacks typically rely on taking advantage of known security vulnerabilities to gain access to systems and encrypt files.

QUESTIONS FOR YOUR ORGANIZATION'S IT STAFF:

» How many members of our IT and non-IT staff have accounts with administrator-level privileges?

» What protective technology gaps exist, and what can our leadership do to help resolve them?

Additional Resources:

National Institute of Standards and Technology (NIST)
csrc.nist.gov

Cybersecurity & Infrastructure Security Agnecy (CISA)
cisa.gov/stopransomware
888-282-0870 | www.cisa.gov

FBI Field Office - Cyber Task Forces
fbi.gov/contact-us/field
Portland Office 503-224-4181
Ransomware Safety Resource

Multi-State Information Sharing and Analysis Center®
(MS-ISAC®) 866-787-4722

Oregon Cybersecurity State Incident Response Team
503-378-5930 | eso.soc@das.oregon.gov

Oregon Emergency Response System
(OERS) 1-800-452-0311

Statewide Interoperability Team
503-373-7251 | swic.or@das.oregon.gov

For more information scan the QR code or visit our website
ransomwareinfo.oregon.gov

ENTERPRISE information services

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.