ENTERPRISE
information services

CYBER SECURITY SERVICES

RANSOMWARE AWARENESS CAMPAIGN

September 2023 | Volume 6

RECOVER

Recover

Recovering from a ransomware incident is a complex and multi-faceted process that can have various outcomes, depending on the organization's level of preparedness, the extent of the damage, and the effectiveness of the recovery efforts.

Data Recovery:

- If the organization has robust and up-to-date backups in place, it can successfully restore encrypted data and systems without paying the ransom, minimizing data loss and downtime.
- Restore systems and data from clean and validated backups.
- Ensure backups are not compromised and are securely stored.

System Validation:

- Thoroughly test restored systems to ensure they are functioning properly and securely.
- Verify that no remnants of ransomware or backdoors remain.

Communication:

- Notify employees, customers, and partners that the situation is under control and systems are being restored.
- Provide any relevant guidance or instructions for using restored systems.

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 – 2:30pm
» October 13, 2023 9am – 10:30am

SOME EXAMPLES OF OUTCOMES WITHIN RECOVER:

» Maintain up-to-date backups to minimize data loss and downtime.
» Conduct an after-action review to gather lessons learned and improve the incident response plan.
» Implement enhanced security measures and improvements to prevent future ransomware attacks.

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.

Monitoring:

- Continuously monitor the restored systems and network for any signs of residual malware or suspicious activities.
- Implement enhanced monitoring to detect and respond to potential reinfections.

Lessons Learned:

- Conduct a post-incident analysis to understand the root causes of the ransomware attack and identify areas for improvement.
- Document lessons learned and insights gained from the incident.

Update Incident Response Plan:

- Use the lessons learned to update and improve your incident response plan for better handling of future ransomware incidents.
- Enhance the plan's recovery procedures, communication strategies, and prevention measures.

Strengthen Security:

- Evaluate and enhance your organization's security posture to prevent future ransomware attacks.
- Implement additional security controls, such as advanced threat detection systems and network segmentation.
- It is important to create a policy about device collection, remediation, and redeployment. You may consider changing Wi-Fi configurations to reduce the odds of reinfection from mobile devices as well as other network configurations.

Continuous Improvement:

- Continuously review and update your recovery procedures based on emerging threats and changes to your organization's IT environment.
- **Participate in industry information sharing to stay informed about new ransomware variants and attack techniques.**

Effective incident response planning, data backup and recovery strategies, and proactive cybersecurity measures are essential for achieving a successful recovery and minimizing the impact of such incidents.

QUESTIONS FOR YOUR IT PERSONNEL:

» Do we maintain offline backups in order to restore systems affected by ransomware?

» Does our disaster recovery plan include recovery time objectives and recovery point objectives for our most mission critical systems?

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.