ankura

ANKURA CYBER THREAT DEFENSE

Ransomware Immediate Response Guide

PREVENTION & RESPONSE

WHAT IS RANSOMWARE?

Cybersecurity incident where malicious actors encrypt files and demand ransom payment to decrypt. Malicious actors may also demand ransom payment to not release stolen data.

WHO DOES THIS AFFECT?

Everyone - Government, Private (profit, non-profit), all industries.

WHY THIS PROBLEM WILL CONTINUE?

Easy money for hard to reach overseas organized cybercrime groups.

PREVENTION BASICS

- Implement anti-phishing email technologies.
- Limit remote access (RDP). Disable unnecessary ports, protocols, and services.
- Implement Multi-Factor Authentication (MFA) for user accounts.
- Conduct phishing awareness education.
- Monitor credentials usage.
- Implement offline backup. Test recovery.
- Implement Nextgen Antivirus (NGAV) and Endpoint Detection and Response (EDR) tools to protect/monitor endpoint devices.
- Implement/review Incident Response Plan (IRP.) Add ransomware playbook.
- Conduct tabletop exercise.
- Review cyber insurance policy.
- Know who to call – Insurance, Breach Counsel, Forensics Firms.

RESPONSE BASICS

- Activate IRP/IRT.
- Identify and contain/isolate affected devices.

  For all affected devices:

  - Backup unencrypted and important files.
  - Restore from clean backup or rebuild.
  - Patch restored/rebuilt systems.
    Scan with advanced AV.
    Power cycle.
  - Connect restored/rebuilt devices back to “clean” network.
  - Install NGAV/EDR.
- Preserve logs.Conduct forensic analysis to identify root cause to improve defense.
- Document.
- Call for assistance if additional help is needed.

Ankura Incident Response Team
incident@ankura.com | 800.496.0089

ankura.com

PROTECT, CREATE, & RECOVER VALUE

Ankura Consulting Group, LLC is an independent global expert services and advisory firm that delivers services and end-to-end solutions to help clients at critical inflection points related to change, risk, disputes, finance, performance, distress, and transformation. The Ankura team consists of more than 1,500 professionals in more than 30 offices globally who are leaders in their respective fields and areas of expertise. Collaborative lateral thinking, hard-earned experience, expertise, and multidisciplinary capabilities drive results and Ankura is unrivaled in its ability to assist clients to Protect, Create, and Recover Value. For more information, please visit: www.ankura.com