SENSEI ENTERPRISES, INC. | CYBERSECURITY RESOURCES

Battle-Tested Strategies:
Tackling Data Breaches and Ransomware Head-On

What is Ransomware?

It is a type of malware (malicious software) that is designed to encrypt files on a device, rendering the files and systems that rely on them unusable or inaccessible.

What is an Incident Response Plan (IRP)?

It is a written document that is approved by senior leadership to assist your organization before, during and after a confirmed or suspected security incident.

It generally outlines the duties and responsibilities of those involved in the process and provides steps and guidance on which key personnel may be need to be involved.

Preparation

a. Maintain offline, user encrypted backups of critical data, and regularly test the ability to restore data and the integrity of backups in a disaster recovery scenario.

b. Ensure that proper policies and plans are in place, followed, and maintained:

  i. Incident Response Plan (IRP)

c. Implement Zero Trust Architecture (ZTA).

  ii. Implementing ZTA will require authentication and authorization before access to a resources is provided.

Prevention and Mitigation

a. Addressing Vulnerabilities and Misconfigurations

  i. Conduct regular vulnerability scans and remediate any discovered vulnerabilities.

  ii. Regularly patch and update software and operating systems to the latest available versions, including third-party software.

  iii. Ensure that all on-premise, cloud services, mobile and personal devices are properly configured and security features are enabled. Including bring your own device (BYOD).

  iv. Limit the use of Remote Desktop programs and services.

b. Compromised Credentials

  i. Implement multi-factor authentication (MFA) for all accounts.

  ii. Consider subscribing to a credential monitoring service to look for compromised credentials.

  iii. Implement identity and access management (IAM) systems.

  iv. Configure inactivity timeouts on computers and mobile devices.

  v. Change default administrator usernames and passwords.

  vi. Do not use administrator accounts for day-to-day operations.

  vii. Implement password policies that require unique passwords of at least 15 characters and utilize password management tools.

  viii. Enforce account lockout policies after a certain number of failed login attempts.

  ix. Disable saving passwords in browsers.

  x. Educate all employees on proper password security in your annual employee security training.

  xi. Separate administrator accounts from standard user accounts.

Prevention and Mitigation

c. Phishing

  i. Implement an employee cybersecurity awareness training program.

  ii. Implement the flagging of external emails in email clients.

  iii. Implement filters at the email gateway to filter out emails with known malicious indicators.

  iv. Enable attachment filters to restrict file types that commonly contain malware.

  v. Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy and verification to assist with mitigating spoofed or modified emails.

  vi. Create a Sender Policy Framework (SPF) DNS record.

  vii. Ensure that macro scripts are disabled for Microsoft Office files transmitted via email.

d. Prior Malware Infection

  i. Use automatic updates for antivirus and anti-malware software and signatures.

  ii. Use application whitelisitng and/or Endpoint Detection and Response (EDR) solutions on all assets so that only allowed software can be run.

  iii. Implement an Intrusion Detection and Intrusion Prevention System (IDS/IPS) to detect potentially malicious activity.

  iv. Monitor for indicators of compromise.

e. Social Engineering

  v. Include social engineering tactics in annual employee cybersecurity awareness training.

  vi. Implement Protective Domain Name System (DNS) to assist in blocking malicious internet activity.

  vii. Consider implementing sandboxed web browsers.

f. Third Parties and Managed Service Providers

  i. Consider the risk management and cyber hygiene practices of third parties or MSPs that your organization relies upon. Ensure that your MSPs or third parties are following best security practices.

  ii. Ensure the use of least privilege and separation of duties when setting up the access of third parties.

  iii. Consider creating service control policies (SCP) for cloud-based resources to prevent users or roles, organization wide, from being able to access specific services or take specific actions within services.

General Best Practices

a. Ensure that your organization has a comprehensive asset management approach. Have an inventory of business IT assets and know which assets are critical to business operations.

b. Keep IT asset documentation stored securely and keep offline backups and physical hard copies.

c. Use the principle of least privilege for all systems and services so users only have access to the items needed to perform their duties.

d. Ensure that systems and services are updated on a regular basis.

e. Use best practices and enable security settings in both local and cloud environments.

f. Employ logical and/or physical network segmentation.

g. Develop and regularly update a comprehensive network diagram to describe systems and data flow in the organization.

h. Restrict usage of PowerShell to specific users on a case-by-case basis utilizing Group Policy.

i. Secure domain controllers (DCs).

j. Retain and secure logs from network devices, local systems, and cloud services, ideally for a minimum of one year when possible.

k. Implement a Security Information and Event Management (SIEM) solution to ingest logs generated by your devices, services and cloud providers to help identify signs of an attack or compromise.

l. Establish a security baseline of normal network traffic and tune network devices to look for abnormal behavior.

m. Conduct regular security and vulnerability assessments.

Detection and Analysis

a. Identify which systems were impacted and isolated them from the network to prevent further damage or spread.

   i. Consider the risk management and cyber hygiene practices of third parties or MSPs that your organization relies upon. Ensure that your MSPs or third parties are following best security practices.

   ii. Prioritize critical systems.

   iii. For cloud resources, take a snapshot of volumes to get a copy for review.

   iv. For physical assets, consider forensic and/or memory imaging.

   v. Utilize out-of-band communications to coordinate isolation of affected services and systems to prevent attackers from learning about the discovery.

b. Power off devices if you cannot disconnect them from the network to avoid the spread of ransomware infection.

c. Triage impacted systems for restoration and recovery.

d. Examine existing organizational detection or prevention systems (antivirus, endpoint detection and response systems, intrusion detection systems, intrusion prevention systems) and log files.

e. Confer with your team to develop and document an initial understanding of what has occurred based on the initial assessment and analysis.

f. Initiate threat-hunting activities, looking for signs of additional compromise or other attack vectors installed by attackers.

Reporting and Notification

a. Follow notificiation requirements outlined in your incident response (IRP) and communicaiton plans.

   i. Keep stakeholders updated and apprised of the situation through regular updates.

   ii. Report the incident to, and possibly request assistance from CISA, local law enforcement or FBI, the FBI Internet Crime Complaint Center (IC3), or local Secret Service office.

   iii. Ensure that when appropriate, coordinate with communications and public relations personnel to be sure that accurate information is shared internally and externally.

b. If the incident resulted in a data breach, follow the requirements outlined in the company IRP and communications plan in conjunction with legal team advice.

Containment and Eradication

a. Create a system image and memory capture of affected devices (computers, servers, etc.)

   i. Preserve evidence that is highly volatile in nature

   ii. Prioritize critical systems.

   iii. Contact your data breach attorney for guidance and legal support.

   iv. Consider reaching out to a digital forensics service provider to assist with the investigation.

b. Consult with federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available to restore access to encrypted data.

c. Research trusted guidance for the identified ransomware variant.

d. Identify accounts and systems that were involved in the breach, including email accounts.

e. Based on the breach or compromise details, contain associated systems that may be used for further or continued unauthorized access.

f. If server-side data is being encrypted by a compromised workstation, follow server-side encryption quick identification steps:

   i. Review computer management sessions and open files lists on associated servers to determine the user or system accessing that resource.

   ii. Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.

   iii. Review remote connection logs and events looking for remote sessions and connections.

   iv. Review Windows security logs, SMB event logs and related logs that may identify significant authentication or access events.

   v. Use packet capturing software on the impacted server with a filter to identify IP addresses involved in the process of accessing or renaming files.

g. Conduct an extended analysis to identify outside-in and inside-out persistence mechanisms. What systems may still be compromised or used in the future to compromise the network again?

h. Reconstruct systems based on their critical importance to operations.

i. Issue password resets for all affected systems and services, address identified vulnerabilities and security gaps.

j. The designated IT security personnel declares when the incident is over based on the criteria outlined in the Incident Response Plan (IRP).

Recovery and Post-Incident Activity

a. Reconnect systems and restore data from offline, user encrypted backups based on priority levels.

b. Document the lessons learned from the incident and the response to the incident

c. Share lessons learned and relevant indicators of compromise with CISA or local ISAC to assist others who may be affected.