Ransomware Protection Guide

1. Prevention Advice - ransomware attack prevention measures

1.1 Precautionary measures – System Protection

(1) Use antivirus software and update the system and applications in a timely manner：Attackers usually use unpatched vulnerabilities to access unauthorized systems and networks to perform subsequent malicious activities.

- Antivirus/antimalware software should be installed and keep updated for the virus and malicious signature code. Perform a scan for the system and network at least once a week, and scan all received documents.
- When a mobile storage device (such as a flash drive) is connected, an antivirus scan should be performed.
- Update the system、application software and firmware to the latest version, also download the latest security update file.

(2) Strengthen the security of the server with dispatch ability: Because the antivirus software has central control on AD server, asset management system, etc. it is necessary to pay special attention to security updates and closely watch their group policies for abnormal changes.

(3) Only enable Microsoft Office macros as needed： Ransomware may infiltrate systems via malicious macros in Word documents. When the victim opens Office, the macro executes, causing the malware to be implanted in the computer.

(4) Minimize open port setting：Ransomware may use exposed services and open ports (such as RDP port 3389 and SMB port 445) to spread on the Internet. In addition to confirming the necessity of opening, it should also be confirmed that the users of these services are trusted.

(5) Set up a firewall to block any network connection with known malicious IP and URL, prohibit the use of rules that allow any connection, and only allow connections with external service IP and DN.

(6) Minimum use authority of personnel：In order to reduce the opportunity for attackers to gain administrative rights, we should:：

- Provide users other than managers with the minimum authority required for their duty, especially accounts that require remote login, such as: RDP.
- View and manage all the usage of user accounts and disable inactive accounts.
- Implement multi-factor authentication.

(7) Raise cyber security awareness：Employees should be trained regularly to establish good cybersecurity awareness and Internet use behavior, such as identifying suspicious e-mails, do not click links randomly, and do not open e-mail attachments from unknown or untrusted sources. In addition, conduct social engineering drills to improve training effectiveness.

(8) System backup：A system backup mechanism should be developed for network-oriented systems to ensure that services can be maintained in the event of a problem with the system.

(9) Enabling the system event log function can provide important evidence when a system failure or abnormality occurs.

1.2 Precautionary measures – Data Protection

(1) Encrypt important and sensitive information：Important and sensitive data should be encrypted. If the data is stolen, it can increase the difficulty for the attacker. In addition, some ransomware only works on common file types (such as images and documents), and encryption can also prevent them from detecting files.

(2) Separate data according to different importance, tasks, etc... Strict access control for important data.

(3) Maintain updated backup and keep them offline：Performing data backup regularly helps to restore data in the event of a ransomware attack, and the host or device storing the backup data should not be connected to the network to prevent the ransomware from affecting the backup data through the network.

- 3-2-1 Backup principle：3 backups, 2 storage media, and 1 offsite storage location.

(4) Regularly maintain image files of important systems：The image file of a virtual machine or server includes a pre-configured operating system and related application software. When an attack occurs and the system needs to be rebuilt, these image files can be used to achieve rapid deployment and recovery.

1.3 Precautionary measurement for enterprise organizations – Preparation for Incident Handling

(1) Before an incident occurs, it is very important to develop an incident contingency plan and conduct drill to verify whether the plan is feasible. When attacked, it is difficult to judge the correct course of action immediately. The plan and implementation will help employees understand the actions to be taken and determine the priority of restoration of various systems and environments.

(2) Prepare a list of external information security units that can seek assistance when a cyber security incident occurs, and a list of police investigations and contact methods.

(3) Join an information sharing organization, such as ISAC or TWCERT/CC.

Reference

[1]https://jenner.com/system/assets/assets/11480/original/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware.pdf
[2]https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf
[3] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks