TLP:WHITE

Ransomware Protection Checklist

Principles for the use of checklists :

Basic item: The general principle for protecting your system from ransomware is to confirm whether the prior technical prevention has been achieved. For the during and after the event, it is recommended as a confirmation for the processing action for completion.

Advanced item: Enterprise has large and complex network environments such as multiple network segments, AD management and control, and virtual platforms, in addition to the basic items needs to be complete, it is also recommended to implement advanced items to achieve a better protection effects; For the consideration on asset, it is important to generate a ranking requirement that can be clarify the sequence of event processing and mitigating the impact for system recovery.

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
1. Prevention Advice	1.1 System protection	1.1.1 Antivirus software	1.1.1.1 Enable real-time virus pattern update function	-	
			1.1.1.2 Full system scan per week	-	
			1.1.1.3 Antivirus software is in the protection state	-	
			1.1.1.4 When a storage device such as a flash drive is connected to the computer, perform an antivirus scan	-	
		1.1.2 Software update	1.1.2.1 Enable automatic security updates for Windows systems	-	
			1.1.2.2 “Update other Microsoft	-	

Ransomware Protection Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
			products" must be enabled in Windows update feature		
			-	1.1.2.3 Confirm the application software update status and keep it up to date	
			1.1.2.4 The OS and application services of antivirus software central control, AD server, and asset management system must be kept up to date	-	
		1.1.3 Group policy	-	1.1.3.1 Regularly confirm whether there are abnormal changes in the group policy or work schedule of the AD server and asset management system	
		1.1.4 Application software	1.1.4.1 Disable the Microsoft office macro and use it only when necessary	-	
		1.1.5 Internet service	1.1.5.1 Perform a network service port scan every quarter, and make sure that each port is turned on for necessary	-	

Ransomware Protection Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
			services, otherwise it should be turned off		
			1.1.5.2 Perform a network service vulnerability scan once a quarter, and correct all high and medium risk vulnerabilities	-	
		1.1.6 Network segmentation	-	1.1.6.1 Implement network segmentation and monitor traffic	
		1.1.7 Firewall	1.1.7.1 Prevent any external connection with known malicious IP and URL	-	
			1.1.7.2 Prohibit the use of rules that allow any connection	-	
			1.1.7.3 Only allow connection with external service IP and DN	-	
		1.1.8 Permission setting	1.1.8.1 Users other than administrators are granted the least privileges to perform tasks	-	
			-	1.1.8.2 View and manage all the usage of user accounts and	

Ransomware Protection Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
				disable inactive accounts	
			-	1.1.8.3 Implement multi-factor authentication	
	1.2 Data protection	1.2.1 Data backup	1.2.1.1 Perform data backup regularly, and the backup interval is not longer than 1 month	-	
			1.2.1.2 According to the 3-2-1 backup principle, 3 backups, 2 storage media, and 1 different storage location	-	
			1.2.1.3 At least one copy of the media or computer used to back up data must be stored in a way that is not connected to the Internet	-	
			1.2.1.4 Adjust the data backup method according to the characteristics of different operating systems (such as Windows, Linux)	-	
		1.2.2 System image	-	1.2.2.1 Important virtual machines and servers should back up image files and follow the data backup rules	

Ransomware Protection Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
		1.2.3 Data encryption	1.2.3.1 Encrypt important data when storing	-	
		1.2.4 Secure access	-	1.2.4.1 Create a list of applications that can access important data	
			-	1.2.4.2 Enable Windows controlled folder access to restrict access to specific folders only by secure applications	
		1.2.5 Asset List	-	1.2.5.1 Inventory of assets and draw up a list of key assets	
	1.3 Cyber security awareness	1.3.1 Education Training	1.3.1.1 Basic cyber security knowledge	-	
			1.3.1.2 Introduction to ransomware attacks	-	
			1.3.1.3 Introduction to phishing attacks, identifying suspicious emails, attached files, links, and web pages	-	
			1.3.1.4 Introduction to social engineering attacks	-	

Ransomware Protection Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
			-	1.3.1.5 Regular social engineering training	
	1.4 Contingency preparation	1.4.1 Contingency planning	1.4.1.1 Plan the division of labor, notification procedures, contact methods, etc. of employees at all levels when an cyber security incident occurs		
		1.4.2 Contingency exercise	-	1.4.2.1 Perform contingency training regularly to confirm the effectiveness	
		1.4.3 Cooperative unit	1.4.3.1 Prepare the list of external information security units, police investigations and contact methods that can be sought for assistance when the information security incident occurs	-	

Ransomware Protection Checklist

Reference

America

https://www.cisa.gov/stopransomware

https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf

https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

https://jenner.com/system/assets/assets/11480/original/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware.pdf

England

https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Cyber Security Companies

https://www.trendmicro.com/en_no/forHome/campaigns/ransomware-protection.html

https://www.nomoreransom.org/zht_Hant/prevention-advice.html