Ransomware Recovery 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
3.Ransomware Recovery	3.1 Device recovery		-	3.1.1 According to the list of key assets and the assessment results of the impact of the hack in 2.2.4.2, prioritize the restoration of assets and the information security protection plan for high-importance assets	
			3.1.2 Reset all passwords and credentials of the device	-	
			3.1.3 Restore using backup data	-	

Ransomware Recovery Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
			3.1.4 Install antivirus software on the restored device and perform a full system scan	-	
	3.2 Share afterwards		3.2.1 Report the incident-related information to TWCERT/CC, assist in sharing it with domestic companies, and prevent more companies from being victimized	-	
			-	3.2.2 Establish an intelligence sharing channel with TWCERT/CC to obtain intelligence information	
	3.3 Review and improve		3.3.1 After responding to the incident, plan and implement corresponding improvement measures at the management level according to the reasons for the hack	-	
	3.4 Data Breach Response		3.4.1 Investigate data breaches using tools like haveibeenpwned, Firefox Monitor, OSRFramework, etc.	-	
			-	3.4.2 Seeking outside security	

Ransomware Recovery Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
				firm to help investigate data breaches in darknet	
			3.4.3 Assess the severity of the C.I.A. of the breached data	-	
			3.4.4 Let internal or external stakeholders understand the incident and provide assistance that can mitigate the impact of the incident	-	

Ransomware Recovery 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