Ransomware Response 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
2.Ransomware Response	2.1 Event confirmation	2.1.1discover and report	2.1.1.1 Self-discovery internally, collect information and submit report	-	
			2.1.1.2 Receive an external abnormal warning or event notification, collect information and submit a report	-	
		2.1.2 Signs of ransomware infection	2.1.2.1 Significant increase in hard disk usage	-	
			2.1.2.2 Significant increase in CPU or memory usage		
			2.1.2.3 The file extension of the affected file has been modified	-	

Ransomware Response Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
			2.1.2.4 The ransom message is displayed on the device screen	-	
		2.1.3 Evaluation decision	2.1.3.1 According to the incident report, evaluate the nature of the incident, and submit it to relevant department personnel based on the result. If confirmed, the response process will be triggered. Item of the assessment of the nature of the event: affected data owner level, Importance of affected data, number of affected hosts, and stakeholder influence, such as customers, product users, etc. (Due to the differences in the nature of the company, this project only provides principled advice)	-	
	2.2 Emergency measures	2.2.1 Prevent expansion	2.2.1.1 Disconnect the infected device from all networks. If it is a sub-domain or multiple devices, disconnect the network from the switch level	2.2.1.2 If the hacked device cannot be disconnected from the network, power off the host. **(This step may affect**	

Ransomware Response Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
				data preservation and evidence maintenance, so use it with caution)	
			-	2.2.1.3 Make sure the mirror server is not infected, and begin the system backup mechanism to maintain the normal operation of system services	
		2.2.2 Report	2.2.2.1 According to the internal notification process of the contingency plan, report to initiate the contingency operation and record the incident	-	
			2.2.2.2 Report the case to the nearest police station with evidence (Take screen shots of online evidence). Or contact Investigation Bureau/Criminal Bureau for assistance. Bureau of Investigation contact information of: service@mjib.gov.tw Criminal Bureau contact information:	-	

Ransomware Response Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
			cib.noransom@cib.npa.gov.tw		
			2.2.2.3 Report cyber security incidents through TWCERT/CC official website (twcert.org.tw) or Email: twcert@cert.org.tw	-	
			-	2.2.2.4 Ensure the confidentiality and security of notifications or external communication channels to prevent alerting attackers	
		2.2.3 Incident assistance	2.2.3.1 Assisted by an external professional information security team	-	
		2.2.4 Impact confirmation	2.2.4.1 Inventory of potentially affected devices, perform antivirus software scans, and confirm whether they are hacked	-	
			-	2.2.4.2 According to the pre-defined list of key assets, evaluate the priority order of the degree of impact of verification	

Ransomware Response Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
			-	2.2.4.3 Monitor network traffic and packets for anomalies	
			2.2.4.4 Inventory the scope of affected data, including: design and development, testing, finance, customers, suppliers, account passwords and other sensitive data	-	
		2.2.5 Event handling	2.2.5 .1 Identify virus types by ransomware name, file extension, etc., and find decryption tools	-	
			2.2.5.2 Confirm the root cause of the information security incident and eliminate it	-	
			-	2.2.5.3 Quarantine backup of affected devices, including encrypted files, databases, etc.	
			-	2.2.5.4 Backup system event log files	
		2.2.6 Stakeholder	2.2.6.1 Let internal or external stakeholders understand the incident	-	

Ransomware Response Checklist

Event Phase	Check Aspects	Sub-aspect	Basic Item	Advanced Item	Status
			and provide assistance that can mitigate the impact of the incident		

Ransomware Response 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