勒索軟體處理檢核表

檢核表使用原則：

基礎項目：企業在防護勒索軟體時的一般性原則，確認事前的技術預防是否已達成，事中、事後則是建議事項或是用在確認處理動作是否遺漏。

進階項目：當較大規模的企業具備多網段、AD 管控、虛擬平台等複雜的網路環境，除基礎項目需達到以外，建議落實進階等級的項目，達成更好的防護效果；同時，在資產方面也產生重要性的排序需求，可快速釐清事件處理順序，提升減輕影響與系統回復的效率。

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
2.事中應變	2.1 事件確認	2.1.1 發現回報	2.1.1.1 內部自行發現，蒐集資訊並提交報告	-	
			2.1.1.2 收到外部異常警告或事件通報，蒐集資訊並提交報告	-	
		2.1.2 感染勒索軟體跡象	2.1.2.1 硬碟使用率大幅提升	-	
			2.1.2.2 CPU 或記憶體使用率大幅提升		
			2.1.2.3 受影響的檔案被修改副檔名	-	
			2.1.2.4 設備螢幕上顯示勒索訊息	-	
		2.1.3 評估決策	2.1.3.1 根據事件報告，評估事件性質，依結果遞交相關部門人員，如經確認，觸發應變流程。 事件性質評估面向為：受影響資料擁有者層級、受影響資料重要性、	-	

勒索軟體處理檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
			受影響主機數量、利害關係人影響性，如客戶、產品使用者等。(此項目因企業性質差異，僅提供原則性建議)		
	2.2 應變處理	2.2.1 防止擴大	2.2.1.1 斷開受感染設備與所有網路的連接，若為 sub-domain 或是多台設備，從 switch 層級斷開網路	2.2.1.2 若無法斷開受駭設備與網路連接，則將主機斷電。**(此步驟可能影響資料保存與證據維護，謹慎採用)**	
		2.2.2 報案與通報	2.2.2.1 依應變計劃之內部通報流程，進行通報以啟動應變作業，並記錄事件經過	-	
			2.2.2.2 向調查局/刑事局報案，尋求協助。 調查局聯絡方式： service@mjib.gov.tw 刑事局聯絡方式： cib.noransom@cib.npa.gov.tw	-	
			2.2.2.3 透過 TWCERT/CC 官網通報(twcert.org.tw)或 Email:twcert@cert.org.tw 進行資安事件通報	-	

勒索軟體處理檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
			-	2.2.2.4 確保通報或對外溝通管道之機密安全性，防範引起攻擊者警覺	
		2.2.3 事件協處	2.2.3.1 由外部專業資安團隊協助處理	-	
		2.2.4 影響確認	2.2.4.1 盤點可能受影響設備，執行防毒軟體掃描，並確認是否受駭	-	
				2.2.4.2 依據預先定義之關鍵資產清單，評估優先查證影響程度的順序	
		2.2.5 事件處理	2.2.5 .1 依勒索軟體名稱、副檔名等分辨病毒類型，尋找解密工具	-	
			2.2.5.2 確認資安事件發生根因，予以排除	-	
		2.2.6 利害關係人	2.2.6.1 讓內部或外部的利害關係人瞭解事件，並提供可減輕事件影響的協助	-	

勒索軟體處理檢核表

參考資料

美國

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

英國

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

資安廠商

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

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