勒索軟體攻擊事後檢核表

檢核表使用原則：

基礎項目：企業在防護勒索軟體威脅時的一般性原則，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
3.事後回復	3.1 設備恢復		-	3.1.1 依據關鍵資產清單及 2.2.4.2 受駭影響評估結果，排定資產恢復優先順序，以及對高重要性資產的資安保護規劃	
			3.1.2 重置該設備的所有密碼、憑證	-	
			3.1.3 使用備份資料進行還原	-	
			3.1.4 重新恢復的設備安裝防毒軟體，並執行全系統掃描	-	
	3.2 事後分享		3.2.1 將事件相關資料通報 TWCERT/CC，協助分享給國內企業，防止更多企業受害	-	
			-	3.2.2 與 TWCERT/CC 建立雙向威脅情資分享機制(如：加	

勒索軟體攻擊事後檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
				入資安聯盟)，進而達到聯防之效。	
	3.3 檢討改進		3.3.1 調查事件發生原因，並依受駭原因，於事件應變後，規劃管理層面對應改善措施並執行	-	
	3.4 資料外洩應變處置		3.4.1 透過 haveibeenpwned、Firefox Monitor、OSRFramework 等工具調查公開資料是否有外洩資料	-	
			-	3.4.2 尋求外部資安公司協助調查暗網是否有外洩資料	
			3.4.3 評估資料外洩的嚴重程度	-	
			3.4.4 通知內外部利害關係人，並提供相關協助	-	

勒索軟體攻擊事後檢核表

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

台灣證券交易所

https://dsp.twse.com.tw/public/static/downloads/listedCompany/%E4%B8%8A%E5%B8%82%E4%B8%8A%E6%AB%83%E5%85%AC%E5%8F%B8%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E7%AE%A1%E6%8E%A7%E6%8C%87%E5%BC%95_final1_20211221111831.docx