勒索軟體防護檢核表

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
1.事前預防	1.1 系統保護	1.1.1 防毒軟體	1.1.1.1 啟用病毒碼即時更新功能	-	
			1.1.1.2 每週 1 次全系統掃描	-	
			1.1.1.3 防毒軟體為啟用防護狀態	-	
			1.1.1.4 隨身碟等儲存設備連接電腦時，應執行防毒掃描	-	
		1.1.2 軟體更新	1.1.2.1 Windows 啟用系統安全性更新的自動更新功能	-	
			1.1.2.2 Windows 更新功能應啟用”更新其它的 Microsoft 產品”	-	
			-	1.1.2.3 確認應用軟體更新狀態，並保持最新狀態	
			1.1.2.4 防毒軟體中控、AD 伺服器、資產管理系統之作業系統與應用服務皆應保持最新的更新狀態	-	

勒索軟體防護檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
		1.1.3 群組原則	-	1.1.3.1 定期確認 AD 伺服器、資產管理系統之群組原則或工作排程，是否有不正常異動狀況	
		1.1.4 應用軟體	1.1.4.1 停用 Microsoft office 巨集功能，僅在必要時使用	-	
		1.1.5 網路服務	1.1.5.1 每季執行 1 次網路服務 port 掃描，並確認每個 port 皆為必要服務所開啟，否則應關閉	-	
			1.1.5.2 每季執行 1 次網路服務弱點掃描，並修正所有高、中風險弱點	-	
		1.1.6 網路分段區隔	-	1.1.6.1 實施網路分段區隔並監控流量	
		1.1.7 防火牆	1.1.7.1 阻止任何與已知惡意 IP、URL 的對外連線行為	-	
			1.1.7.2 禁止使用允許任何連線的規則	-	
			1.1.7.3 只允許與對外服務的 IP、DN 進行連線	-	
		1.1.8 權限設定	1.1.8.1 管理者以外使用者，給予可執行工作之最小權限	-	

勒索軟體防護檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
			-	1.1.8.2 查看和管理所有使用戶帳戶的使用情況，並禁用非活動帳戶	
			-	1.1.8.3 實施多因子身份認證	
	1.2 資料保護	1.2.1 資料備份	1.2.1.1 定期執行資料備份，且備份間隔不長於 1 個月	-	
			1.2.1.2 依照 3-2-1 備份原則，3 份備份、2 種儲存媒體、1 個不同的存放地點	-	
			1.2.1.3 資料備份所存在的媒體或電腦，至少有 1 份以未連接網路的方式存放	-	
			1.2.1.4 依不同作業系統(如 Windows、Linux)特性調整資料備份作法	-	
		1.2.2 系統映像檔	-	1.2.2.1 重要的虛擬機與伺服器應備份映像檔(image file)，且比照資料備份規則執行	
		1.2.3 資料加密	1.2.3.1 對重要資料存放時應進行加密	-	

勒索軟體防護檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
		1.2.4 安全存取	-	1.2.4.1 建立可存取重要資料的應用程式清單	
			-	1.2.4.2 啟用 Windows 受控資料夾存取功能(controlled folder access)，限制只有安全的應用程式才能存取特定資料夾	
		1.2.5 資產清單	-	1.2.5.1 盤點資產，並訂定關鍵資產清單	
	1.3 資安意識	1.3.1 教育訓練/演練	1.3.1.1 基礎資安知識	-	
			1.3.1.2 勒索軟體攻擊介紹	-	
			1.3.1.3 釣魚攻擊介紹，識別可疑郵件、附檔、連結、網頁	-	
			1.3.1.4 社交工程攻擊介紹	-	
			-	1.3.1.5 定期進行社交工程演練	
	1.4 應變準備	1.4.1 應變規劃	1.4.1.1 規劃資安事件發生時，各層級員工分工、通報流程、連絡方式等		
		1.4.2 應變演練	-	1.4.2.1 定期執行應變演練，確認成效	

勒索軟體防護檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
		1.4.3 協處單位	1.4.3.1 準備資安事件發生時，可尋求協助的外部資安單位、警調之清單與連絡方式	-	
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、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)	-	

勒索軟體防護檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
	2.2 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	-	
			-	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	-	

勒索軟體防護檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
			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	-	
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	-	

勒索軟體防護檢核表

事件階段	檢核面向	子面向	基礎項目	進階項目	檢核欄
			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	-	
	3.3 檢討改進		3.3.1 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	-	

勒索軟體防護檢核表

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