



高級中等學校使用亞昕公司所開發之單 機版校務行政系統遭駭客竊取及洩漏個 人資料事件辦理情形

報告機關：教育部

113年12月25日

限閱：行政院資安會報第44次會議資料公開簡報



大綱

1

基本資訊

2

事件發生經過及辦理進度說明

3

調查事實整理個案調查綜合分析、建議與結論



1

基本資訊

限閱：行政院資安會報第44次委員會議-會前公開簡報



基本資訊

報告機關

教育部

執行行政 調查機關

- 教育部國民及學前教育署(以下稱本部國教署)
- 臺中市、臺南市、桃園市政府

協助調查之機關 行政法人或團體

中華資安國際股份有限公司(以下稱中華資安)、財團法人資訊工業策進會(數位發展部數位產業署協助)



2

事件發生經過及 辦理進度說明

限閱：行政院資安會報第44次委員會議-會前公開簡報



事故發生原因分析

- 本事件經初步調查發現，高中之校務行政系統主機存有高度資安風險，遭駭客成功登入、執行惡意程式並取得資料庫特權權限，並利用竊取之資料再登入其他高級中等學校。

限閱：行政院資安會報第4期
會前公開簡報



第一時間採取應變措施

本部國教署於本事件發生後，即於第一時間通知受害學校及臺中市政府教育局進行下列各項緊急應變作業：

1	將受駭伺服器離線（拔除網路線）及保持開機（勿重新開機）
2	於新的主機環境重灌應用系統，並維持原始狀態
3	確認新主機環境與既有主機環境已完全進行網段區隔
4	變更所有伺服器帳號密碼
5	儘速配合本部國教署進行安全性檢測
6	建議洽詢專業技術資安公司，辦理數位鑑識，釐清事件原因及損害程度



3

個案調查綜合分析、 建議與結論

限閱：行政院資安會報
行政院資安會報-會議-會前公開簡報



個案調查綜合分析、建議與結論

經調查發現，部分私立學校管理之校務行政系統主機及使用之單機版校務行政系統存在資安風險，爰本部國教署、臺中市政府教育局及亞昕公司將共同合作，協助使用該版本之學校辦理以下事項：

- 協助全國高級中等學校停止使用Client server版本校務行政系統，並轉換使用web版校務行政系統。
- 持續協助學校落實校務行政系統主機管理，以降低系統受駭之風險。
- 協助私立高級中等學校依據個人資料保護法第27條及「私立高級中等以下學校及幼兒園個人資料檔案安全維護計畫實施辦法」規定，訂定「個人資料檔案安全維護計畫」，並落實執行。
- 持續強化學校對於系統之資通安全與個人資料保護能力，並提升教職員工生防詐意識。



持續落實校務行政系統主機管理

持續提升主機及系統資安防護能力，包括：

1	所有作業系統、防毒軟體和應用程式(Adobe Reader、Java、7zip等)、瀏覽器(Chrome、Edge等)皆應保持在最新版本
2	移除不安全軟體(如flash、rar等)
3	辦理主機及網頁弱點掃描，並修補中風險以上弱點
4	密碼資料表加密，並確認登入頁面傳送為加密連線
5	主機及應用系統辦理帳號清查作業(所有帳號含管理者、使用者等)
6	重新檢視系統、主機之帳密複雜度、長度及變更週期，並評估移除閒置帳號(將超過6個月未登錄帳號移除/停用)，並以最小權限原則開放
7	SQL Sever 預設port(1433)關閉，改用其他port
8	廠商連線來源IP要在學校防火牆設定規則限制
9	資料庫預設帳號SA應停用及系統後臺提供雙重驗證機制



報告完畢敬請裁示

限閱：行政院資安會報第44次會議-會前公開簡報