調查結果

根據香港法例第 486 章《個人資料（私隱）條例》第 48(2)條發表

香港桂冠論壇委員會的
資訊系統遭勒索軟件攻擊

背景

個人資料私隱專員公署（私隱專員公署）已就香港桂冠論壇委員會（桂冠論壇）通報的一宗資料外洩事故完成調查。

調查源於桂冠論壇於 2023 年 9 月 27 日向私隱專員公署通報資料外洩事故，表示桂冠論壇的電腦系統及檔案伺服器遭受勒索軟件攻擊（外洩事件）。

調查發現桂冠論壇的網絡最初於 2023 年 9 月 26 日遭黑客入侵。黑客透過暴力攻擊取得桂冠論壇一個具系統管理員權限的帳戶（該帳戶）憑證，並利用該帳戶通過防火牆的虛擬私有網絡區域成功進入桂冠的伺服器。黑客隨後於桂冠論壇的網絡內進行橫向移動及放置勒索軟件「Elbie」，導致儲存在桂冠論壇的一組伺服器及七個端點裝置的檔案被加密。同時，存放於另一組伺服器的備份數據亦遭黑客毀壞。

受外洩事件影響的人士數目為 8,122 名，包括約 7,200 名電子通訊訂閱戶的姓名及電郵地址受影響，另外約 920 名的受影響人士包括青年科學家申請人、邵逸夫獎得獎者及其隨行人員、論壇大使／活動助理申請人、本地科學家及講者、評審員、活動助理，以及桂冠論壇的現職僱員、前僱員及委員。涉及的個人資料包括姓名、地址、電郵地址、電話號碼、護照資料、完整及／或部分護照／香港身份證號碼、銀行戶口／信用卡資料、出生日期、國籍／出生地、履歷表／成績單、關聯機構及／或學歷背景。

桂冠論壇在外洩事件發生後採取了多項機構性和技術性的改善措施，包括重新訂定防火牆規則，進行全面的帳戶審計及制定嚴格的密碼政策等，以提升整體系統保安以保障個人資料私隱。

調查結果

經考慮外洩事件的情況及調查所獲得的資料，個人資料私隱專員（私隱專員）鍾麗玲認為桂冠論壇的以下缺失是導致外洩事件發生的主因：－

1. **資訊系統管理有欠妥善**，包括其防火牆的韌體已過時並存在多項嚴重漏洞、防毒軟件的病毒資料庫自 2019 年起不曾更新、沒有為遠端存取資料啟用多重認證功能核實用戶身分、沒有制定密碼政策、沒有採用網絡分段或設置內部防火牆規則，亦不曾為資訊系統進行保安審計及漏洞評估等；

2. **對服務供應商採取的資料保安措施缺乏監察**，以確保服務供應商履行已簽訂的合同要求適時更新軟件及安裝修補程式，導致桂冠論壇在外洩事件發生後才發現其防火牆使用已過時的韌體並存在多項嚴重漏洞，而防毒軟件的病毒資料庫亦已過時；

3. **欠缺資訊保安政策及指引**，令員工及服務供應商未能清楚了解他們在網絡保安框架下的責任及需實施的安全規程；及

4. **缺乏適當的數據備份方案**，未有將原始數據及備份數據存放於不同網絡，導致備份數據在外洩事件中遭黑客毀壞，無法進行數據復原。

私隱專員的決定

基於上述原因，私隱專員鍾麗玲裁定桂冠論壇沒有採取所有切實可行的步驟以確保涉事的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，因而違反了《個人資料（私隱）條例》的保障資料第 4(1)原則有關個人資料保安的規定。

私隱專員已向桂冠論壇送達執行通知，指示其採取措施以糾正違規事項，以及防止類似違規情況再次發生。

鍾麗玲
個人資料私隱專員
2024 年 8 月 8 日