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

香港芭蕾舞團有限公司的伺服器遭勒索軟件攻擊

背景

個人資料私隱專員公署（私隱專員公署）已就香港芭蕾舞團有限公司（芭蕾舞團）通報的一宗資料外洩事故完成調查。

調查源於芭蕾舞團於 2023 年 10 月 16 日向私隱專員公署通報資料外洩事故，表示芭蕾舞團於 2023 年 9 月 29 日遭受勒索軟件攻擊，導致其資訊系統的四組實體伺服器受影響（外洩事件）。

調查發現芭蕾舞團的網絡最初於 2023 年 9 月 15 日遭黑客入侵。由於當時芭蕾舞團的一組伺服器的運作軟件已屬過時，黑客遂利用該伺服器的漏洞，成功進入芭蕾舞團的網絡。黑客隨後透過各種惡意工具及程式，包括轉儲憑證工具及遠端存取工具，在取得資訊科技管理員及用戶的帳戶密碼後，進而獲取了與芭蕾舞團的網絡的相關資料及與網絡連接的電腦的詳情，並在其網絡內進行橫向移動。

黑客於 2023 年 9 月 17 日利用一個系統管理員帳戶，放置勒索軟件「LockBit」，導致儲存在芭蕾舞團資訊系統內的檔案被加密，黑客並竊取了系統內的資料及檔案。

調查亦發現，芭蕾舞團無法確實受影響檔案內的資料。根據芭蕾舞團的估算，受外洩事件影響的人士數目可能為 37,840 名，包括芭蕾舞團的僱員、求職者、門票訂購者、客席藝術家、活動參加者、捐款者、贊助者及供應商。涉及的個

人資料包括姓名、香港身份證號碼、護照號碼、相片、出生日期、地址、電郵地址、電話號碼、健康資料、銀行戶口號碼及／或信用卡號碼（不包含安全碼）、僱傭資料及學歷資料。

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）鍾麗玲認為芭蕾舞團的以下缺失是導致外洩事件發生的主因：—

1. **相關伺服器的運作軟件已過時**，並存在多項嚴重的遠端程式碼執行漏洞，而芭蕾舞團沒有任何關於保安修補或更新其伺服器的政策或程序，這突顯了芭蕾舞團在定期保安修補及更新方面的明顯缺失；

2. **相關伺服器在服務供應商進行系統遷移過程中被不必要地曝露於互聯網**，大幅增加遭受網絡攻擊的風險，亦使相關伺服器在外洩事件中遭黑客利用；

3. **對服務供應商採取的資料保安措施缺乏監察**，以確保服務供應商對系統作出適時更新，並對資訊系統實施足夠的保安措施以保障儲存在內的個人資料，而與服務供應商簽訂的服務合約中，亦沒有關於資料保安方面的要求；及

4. **沒有對資訊系統進行保安評估及保安審計**，導致芭蕾舞團未能適時識辨相關伺服器的漏洞，亦增加了資訊系統受到攻擊的風險。

私隱專員的決定

基於上述原因，私隱專員鍾麗玲裁定芭蕾舞團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。

私隱專員已向芭蕾舞團送達執行通知，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