消委會遭網襲 逾450人資料外洩

私隱專員揭五大缺失 猶如「裝鎖不上鎖」任黑客自出自入

香港消費者委員會的電腦系統去年9月被黑客攻擊並遭勒索，個人資料私隱專員公署昨日發表調查報告，指此次事件中，超過450人的個人資料外洩，包括投訴人、資訊科技服務供應商的員工以及消委會現職及已離職的員工。公署批評消委會存在五大不足，包括疫情期間容許員工居家工作，卻沒有為遠端存取資料庫啟動「多重認證」功能，導致黑客能取得賬戶憑證後，輕易進入網絡。該會雖然已安裝網絡安全軟件，但竟沒有開啟軟件，「猶如有安裝門鎖卻沒有上鎖」，導致系統未能偵測及攔截，黑客自出自入網絡系統逾兩周才發現。專家提醒，居家工作漸普遍，不少香港企業機構容易出現網絡漏洞，對網絡安全需提高警惕（見另稿）。

◆香港文匯報記者 吳健怡

▶私隱專員揭露消委會在網安方面存在五大不足。 香港文匯報記者曾興偉 攝

黑客入侵、勒索消委會經過

2020年5月起 消委會使用網絡安全軟件，以偵測及攔截網絡安全威脅，遇有襲擊會向消委會發出警報。但是消委會沒有啟動以及妥善設定該網絡安全軟件，導致軟件未有發揮偵測及攔截作用。

2020年11月 消委會實施居家工作安排，允許員工透過VPN遠端連接消委會的網絡，但是考慮到員工對採用多重認證功能的阻力及資訊部人手不足，未有為遠端存取資料啟用多重認證功能，以核實授權才可遠端登入消委會網絡。

2022年5月 消委會取消居家工作安排，但仍允許員工在沒有多重認證情況下，遠端連接消委會的網絡。

2023年6月起 有289名投訴的個人資料，因人為錯誤或疏忽，被儲存於沒有配置網絡安全軟件的一個測試伺服器內，以及未有於系統內設定一個複雜密碼。

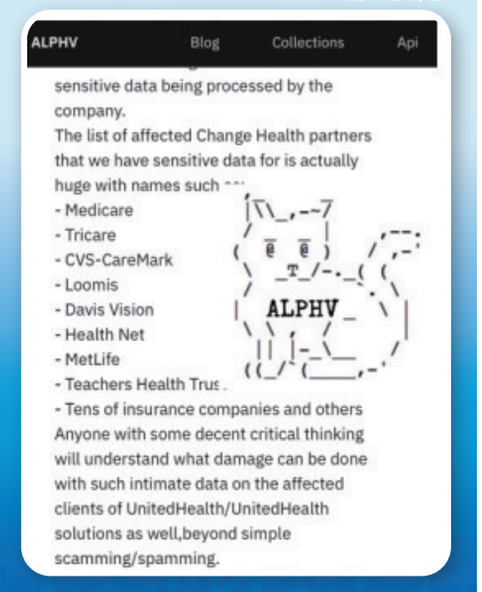
2023年9月4日 黑客組織ALPHV獲取並利用消委會一個具管理員權限的賬戶，透過虛擬私有網絡(VPN)進入消委會的網絡。

2023年9月19日及20日 消委會伺服器及端點裝置遭受到勒索軟件攻擊。

2023年9月21日 消委會向公署通報該事件。

資料來源：個人資料私隱專員公署
整理：香港文匯報記者 吳健怡

▼圖為入侵消委會網絡的黑客組織ALPHV在炫耀過去攻擊海外醫療機構的「戰績」。 網上圖片



黑客組織ALPHV去年9月4日獲取並利用消委會一個具管理員權限的賬戶，透過虛擬私有網絡（VPN）進入消委會的網絡，導致消委會的93個系統遭到惡意加密，11個伺服器及端點裝置被黑客入侵，其間警報系統一直沒有發出警示。

同年9月20日，消委會發現其伺服器及端點裝置遭受勒索軟件攻擊；及後在9月21日，消委會向公署通報事件。

參與調查的網絡安全專家證實，事件涉及的數據少於1.5GB，4個載有個人資料的檔案遭受未獲准許的查閱，涉及超過450人的個人資料：包括投訴人（289人）、資訊科技服務供應商的員工（26人）、消委會的現職（138人）及已離職員工（24人）。資料包括姓名、手提電話號碼、住宅或通訊地址、電郵地址、收入範圍等。

私隱專員鍾麗玲指出消委會有五大缺失導致事故，其中最大原因是消委會沒有為遠端存取資料啟用多重認證功能，導致黑客能利用獲取的賬戶憑證進入消委會的網絡、進行勒索軟件攻擊。

她指出，由於消委會2020年11月疫情期間為方便員工在家工作，容許員工透過VPN連接消委會網絡，而未有啟用多重認證核實身份，直到2022年取消居家工作安排，仍允許員工在沒有多重認證功能的情況下進行遠端連接消委會的網絡，事發後始暫停該安排。

有開安全軟件雞蛋同放一籃

鍾麗玲指出，消委會另一缺失是沒有妥善設定用作偵測及攔截網路安全威脅的網路安全軟體，雖然消委會早於2020年5月已安裝網絡安全軟件，卻未有啟動該軟件的警報功能，令該網絡安全軟件未能在檢測到網絡安全威脅後發出警報電郵。

她又指，導致今次事件的另一個主要成因，為消委會欠缺足夠保安措施禁止或防止於測試伺服器內儲存真實的個人資料。

她表示，有289名投訴人的個人資料因人為錯誤或疏忽，自2023年6月起被儲存在沒有配置網絡安全軟件的測試伺服器內，「一般來說，考慮到測試伺服器保安措施一般都比較薄弱，我們認為機構不應將真實個人資料儲存在測試的伺服器內。」

調查亦發現一名前資訊科技部員工沒有於系統設定複雜密碼政策，令有關政策在事發時未有被貫徹實施。

消委會五大缺失

1. 沒有爲遠端存取資料啟用多重認證功能
2. 沒有妥善設定用作偵測及攔截網絡安全威脅的網絡安全軟件
3. 欠缺足夠保安措施禁止或防止於測試伺服器內儲存個人資料
4. 資訊保安政策有欠全面及具體
5. 保障個人資料私隱及網絡安全意識不足

資料來源：個人資料私隱專員公署
整理：香港文匯報記者 吳健怡

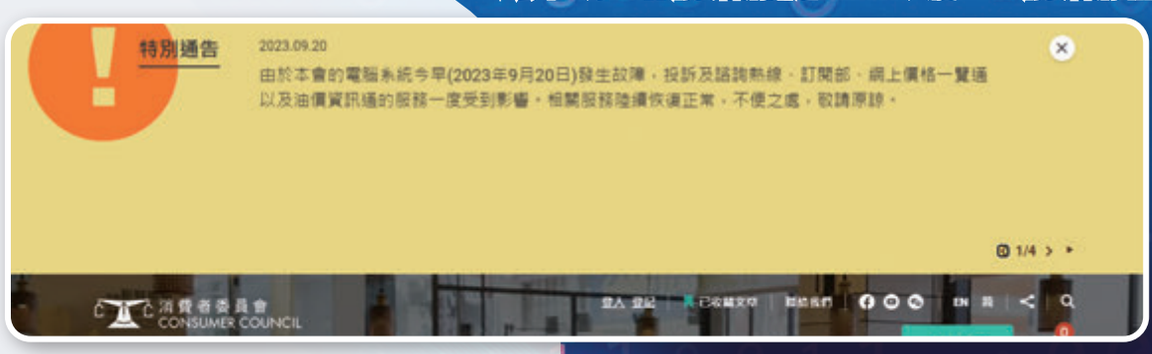
未明黑客如何奪管理員權限

至於黑客是如何取得具管理員權限的賬戶？鍾麗玲坦言，相關員工及消委會亦「解釋唔到」，故私隱專員亦「理解唔到」。

鍾麗玲批評，消委會在保障個人資料及網絡安全意識不足，亦欠缺全面和具體的資訊保安政策，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《個人資料(私隱)條例》第4(1)原則。

私隱專員公署首席個人資料主任（合規及查詢）郭正熙表示，暫時共接獲20宗相關查詢及8宗投訴，向消委會發出7項執行指令，包括要求為所有遙距存取載有個人資料的系統實施多重身份認證、聘請獨立資訊安全專家檢視資訊系統保安措施、定期檢視資訊系統的保安措施、制訂清晰全面的政策，以禁止在測試伺服器內儲存個人資料等。他續指，現已向消委會送達執行通知，指示糾正其違反事項，要求兩個月內、即6月29日須提交證據證明已執行，否則屬違法，公署會跟進。由於消委會通報處理及時，暫不會就事件作出檢控。

▼去年9月20日消委會網絡遭ALPHV入侵。 消委會網站截圖



機構犯錯成本低 宜加罰「督促」改正

專家之言

有電腦安全專家昨日對香港文匯報指出，香港個人私隱專員公署只能針對事件調查和警告，只要涉事企業及機構改善問題，便沒有刑責，但受影響市民的個人資料可能已經在暗網上被人販賣。「香港寬鬆的法例令企業及機構有改過的機會，犯錯成本好低，有些企業因此漠視網絡安全的問題。」鑒於居家工作漸普遍，企業機構對網絡安全須提高警惕。

同類案例 星予重罰

根據香港《個人資料（私隱）條例》，私隱專員可向證實違規者發執行通知要求糾正，違反該執行通知的話，才會構成刑事罪行，最高罰款5萬元及監禁兩年，另加每日罰款1,000元；重犯者最高可被判罰款10萬元及監禁兩年，加每日罰款2,000元。相比之下，新加坡法例十分重視個人資料外洩的問題，一旦發生網絡安全事故，相關罰款高達100萬新加坡幣（約合港幣575萬元），或該公司當年的10%收入。不少香港電腦安全專家認為，香港「私隱條例」亦應該加重罰則，使企業及機構明白罰款嚴重，才會重視網絡安全。

至於消委會今次事故，據悉該會本身設有資訊科技部，並在黑客入侵事故前，聘請網絡專家定期為系統進行檢測，惜最終仍是百物一疏，到底問題出在哪裏？香港智慧城市聯盟資訊科技管理委員會主席龐博文分析，事件揭露消委會系統陷入「網絡不設防」危機，雖有資訊科技部門，但監察及抵禦入侵的能力有待改善：「不少企業或機構會以為只要公司設有資訊科技部就可以解決一切跟網絡有關的奇難雜症，其實不然，情況就等如地盤有一批手爪起腱的大隻佬也沒有用，一旦沒有聘請保安員，夜深人靜一樣可以遭人入侵。」

龐博文認為消委會經此一役後，有必要全面提升系統使用者、管理者及服務供應商的網絡安全意識及應變能力：「作為企業或機構的負責人，自己必須具備一定網絡保安知識，這樣才懂得分辨服務供應商的優劣，否則連要求也不懂得提出，也不懂得如何監察，請了網絡保安公司也不代表抵禦能力到位。」

◆香港文匯報記者 文禮願

消委會：已啟用多重認證 完善指引增培訓

香港文匯報訊 消費者委員會昨日回應指，對私隱專員公署提出的具體建議及批評，消委會深表重視，在事故發生後已積極採取即時行動糾正問題，當中包括為遠端存取資料啟用多重要素認證（MFA）功能、全面檢視網絡安全方案的功能及作出妥善設定，及進一步加強內部培訓以提升員工對網絡安全的意識和行為。

根據外聘的暗網監察服務商的資料，至目前為止未有發現任何受影響的消委會資料被公開。

消委會表示，現時亦正完善其資訊科技政策和工作指引，同時正委託威脅偵測與應變服務供應商，以加強抵禦網絡保安威脅的能力。在發現事故後，消委會即時採取相關遏制行動，以保護並恢復資訊科技系統；委託鑑證專家檢查系統，深入調查事件起因和資料是否有被盜取，並根據專家意見作出遏制和強化行動，加強資訊科技保安措施以防止黑客再次入侵；再三確認鑑證調查結果後，以負責任的態度向受影響人士發出個別通知，及向不受影響的人士發出更新通知以釋疑慮，以及委託服務商全天候監察暗網，以便第一時間知悉是否有被盜取的資料被公開。

黑客勒索如無底洞 暗網幾千元賣隱私

黑客盜取企業或機構的網絡資料後，大多會放上「暗網」（Deep Web）兜售。香港文匯報記者發現，黑客出售的個人資料不乏香港身份證正反兩面資料、號碼及手提電話號碼等。近日有黑客正兜售一批聲稱是香港身份證號碼的資料，索價399美元，折合約爲3,100港元。

私隱專員鍾麗玲亦指出，資料外洩已經成爲全球性問題，個人資料又是「有價有市」，若公司或機構缺乏網絡安全管理，便容易遭到黑客攻擊，導致大量個人資料遭遇洩露、被倒賣，形成黑色產業。

交贖金照「撕票」資訊防護不能慳

她指出，網絡罪犯除了透過網絡攻擊，將客戶的個人資料轉售予關連機構作推廣用途外，亦試圖獲取金錢利益，利用竊取的資料盜用他人身份或達到其他欺詐目的。以今次消委會爲例，於去年9月曾交代，電腦系統遭黑客入侵，被勒索50萬美元至70萬美元贖金，但是消委會並未交付贖金。她提醒，絕對不要繳交贖金，「即使畀咗錢亦不代表個人資料可以取還。」她又強烈譴責黑客於網絡世界的非法活動。

經歷了全球疫情的衝擊，「遠程工作」不僅是許多企業在疫情期間的解決之道，也一直延續到疫後的現在，但卻暗藏黑客攻擊的危機。鍾麗玲認爲，疫情而引致「遠程工作」或「在家工作」的安排是現時新趨勢，但有關安排涉及遙距登入資訊系統，有多一重風險，需注意網絡安全。她呼籲，對遙距登入資訊及通訊系統使用多重身份驗證，各機構需要考慮涉及的數據是否包含個人資料，是否敏感、數量多少，再決定是否應加大保障，例如傳輸時是否需要加密，以及設立雙重認證安排。

私隱專員公署建議，爲保證數據安全，不論大小企業「都唔好慳錢」，投放適當資源在資訊安全方面，特別是客戶的個人資料，包括設定穩健的網絡保安框架、定期對資訊系統進行風險評估及保安審計、建立重視數據安全的企業文化及建立有效的培訓計劃，加強員工對保障個人私隱的意識和能力。

◆香港文匯報記者 吳健怡