SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

2020 年 4 月 29 日

致持牌法團的通函

與遙距工作安排相關的網絡保安風險管理

鑑於愈來愈多公司採用遙距工作安排，證券及期貨事務監察委員會（證監會）提醒持牌法團須評估其操作能力，及實施適當的措施以管理與這些安排相關的網絡保安風險。

當員工以遙距方式工作時，可能會從辦事處以外的地點接達持牌法團的內部網絡和系統，及透過視像會議平台舉行會議。本通函就監控措施及程序列舉了多個例子，以協助持牌法團保護內部網絡和數據。持牌法團務請注意，以下例子並非詳盡無遺。持牌法團應實施並維持就相關情況而言被視為適當且與其業務的規模和複雜程度相稱的措施[1]。

(A) 遙距接達內部網絡和系統

近期，某持牌法團所匯報的一宗網絡保安事故顯示，網絡罪犯如何利用虛擬私有網絡（Virtual Private Network，簡稱 VPN）軟件[2]在市場上的已知漏洞，入侵該持牌法團的網絡、存取客戶數據及發出未經授權而轉移資金的指示。

用以紓減與遙距接達相關的網絡保安風險的適當監控措施及程序可以包括：

- 實施穩健的 VPN 解決方案，藉以提供強效的加密程式及兩重或以上的防護，以保障在遙距使用者裝置與內部系統之間傳輸的數據的完整性；
- 使用多個 VPN 伺服器以提供額外保障；
- 及時監察、評估及執行 VPN 軟件提供者發布的保安修補程式或修正程式[3]；
- 規定僱員、代理和服務提供者須使用難以破解的登入密碼來進行遙距接達，及實施雙重認證[4]，尤其是在接達特權帳戶及敏感數據庫時；
- 避免向外界人士授出常設或永久接達權，及只容許系統供應商在預設的時段內接達特定的系統；
- 實施不同級別的遙距接達，例如持牌法團所提供的電腦和流動裝置配備比僱員私人擁有的裝置更大的操作能力；

---

1 《證券及期貨事務監察委員會持牌人或註冊人操守準則》第 4.3 段規定，持牌法團須設有妥善的內部監控程序、財政資源及操作能力，而按照合理的預期，這些程序和能力足以保障其運作、客戶或其他持牌人或註冊人，以免其受偷竊、欺詐或不誠實的行為、專業上的失當行為或不作為而招致財政損失。此外，《適用於證券及期貨事務監察委員會持牌人或註冊人的管理、監督及內部監控指引》第 IV 部規定，持牌法團須確保所有與其業務運作有關的資料（包括以文件及電子方式儲存的數據）都是完整、連貫、保密、齊備、可靠和詳盡的，及確保運作及資料管理系統均配合公司的需要，並在保密及有充分監控的環境下運作。

2 VPN 透過互聯網提供由遙距裝置至內部網絡的加密連接，有助確保敏感數據在傳輸過程中得到保護。

3 多個資訊科技保安專業組織已就 VPN 軟件中未修補的漏洞提出關注，這些漏洞容易被黑客利用，危害受害者的網絡。

4 雙重認證指使用以下任何兩項元素的認證機制：客戶所知的、客戶所有的及客戶是誰。

- 實施保安監控措施，以防止有人在未經授權的情況下在提供給員工的電腦和裝置內安裝硬件和軟件；及

- 實施穩健的網絡隔離措施，以根據關鍵程度來分隔系統伺服器及數據庫，從而加強保護較為關鍵和敏感的數據，例如客戶個人資料。

(B) 使用視像會議平台

與視像會議平台相關的保安問題時有報道。為了紓減有關未經授權的接達及洩漏關鍵或敏感數據的風險，適當的監控措施及程序可以包括：

- 在使用視像會議平台之前，評估其保安特點；

- 規定參與者須登記方可出席視像會議；

- 透過查核使用者的電郵地址或利用“等候室”功能[5]等方式，只允許經認證及獲授權的使用者加入視像會議；

- 使用隨機的會議編碼，而非個人會議編碼；

- 透過會議軟件或其他合法途徑（例如辦事處電郵）邀請參與者，並避免藉社交媒體帖文分享會議連結；

- 在視像會議平台上啟用密碼保護功能；

- 在適當情況下，於所有參與者加入後閉鎖會議；及

- 使用最近期版本的軟件，並安裝最新的保安修補程式。

(C) 其他支援遙距工作安排的措施

此外，持牌法團應在適當情況下制定以下措施，藉以提升操作能力，及監察各項遙距工作的機制：

<u>系統能力</u>

- 評估現有的資訊科技基礎設施、軟件（例如遙距電腦裝置、網絡頻寬及軟件許可證）及硬件（例如手提電腦及流動裝置）就支援遙距工作安排而言是否足夠，並對其加以改進。

<u>監察及事故處理</u>

- 實施監察機制，以偵測未經授權而接達內部網絡和系統的情況，例如檢視未經授權的接達嘗試的列表，及偵測使用未經批准的應用程式的情況；及

- 制定並維持有效的事故管理與匯報機制。

[5] “等候室”功能讓視像會議的主持人可只准許獲授權的參與者加入會議。

網絡保安培訓及警示

- 向所有內部系統使用者提供充分的網絡保安培訓，及定期向客戶發出適當的提示和警示，例如有關防範性保安措施的意見，新冒起的網絡保安威脅和趨勢（例如仿冒詐騙[6]及勒索軟件），以及使用安全的無線網絡來接達內部網絡和視像會議平台。

如對本通函的內容有任何疑問，請聯絡你的個案主任。

證券及期貨事務監察委員會
中介機構部
中介機構監察科

完

SFO/IS/018/2020

[6] 仿冒詐騙是指黑客試圖誘騙使用者犯錯，例如點擊會下載惡意程式的連結，或將他們導引至欺詐網站。