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

SFC
證監會

《降低及紓減與互聯網交易相關的黑客入侵風險指引》

目錄

引言

1. 本指引由證券及期貨事務監察委員會（證監會）根據《證券及期貨條例》第 399 條發表，當中載明了有關降低或紓減與互聯網交易相關的黑客入侵風險的基本規定。

2. 本指引應連同（除其他條文外）《證券及期貨事務監察委員會持牌人或註冊人操守準則》（《操守準則》）第 18.4 至 18.7 段、附表 7 第 1.1、1.2.2 至 1.2.8、1.3 及 2.1 段一併閱讀。就本指引而言，“互聯網交易”一詞的涵義與《操守準則》第 18.2(f)段所界定者相同，即“透過持牌人或註冊人以互聯網為基礎的交易設施向該持牌人或註冊人傳送交易指示的安排”。

3. 本指引適用於從事互聯網交易，並就以下活動獲證監會發牌或註冊的人：

   - 第 1 類受規管活動（證券交易）；
   - 第 2 類受規管活動（期貨合約交易）；
   - 第 3 類受規管活動（槓桿式外匯交易）。為免生疑問，本指引只適用於獲證監會發牌的槓桿式外匯交易商；及／或
   - 第 9 類受規管活動（提供資產管理），惟以那些以其互聯網為基礎的交易設施分銷所管理的基金者為限。

4. 本指引並無法律效力，亦不應以任何方式被詮釋為可以凌駕於任何適用法律、守則或其他監管規定的條文。然而，任何人如未能遵從本指引的精神，則可能對其適當人選資格造成負面影響。

5. 本指引訂明的監控措施僅可降低或紓減與互聯網交易相關的黑客入侵風險，無法消除有關風險。必須強調的是，該等監控措施只是持牌人或註冊人應達致的最低標準，及並非詳盡無遺。持牌人或註冊人應實施與其架構、業務運作及需要相稱而足夠及有效的措施。

1. 保護客戶的互聯網交易帳戶

1.1. 雙重認證[1]

持牌人或註冊人應就客戶的互聯網交易帳戶的登入程序實施雙重認證。

持牌人或註冊人應評估及實施與其業務模式相稱的雙重認證解決方案。

1.2. 實施監察及監督機制

持牌人或註冊人應實施有效的監察及監督機制，以偵測未經授權而接達客戶的互聯網交易帳戶的情況。

[1] 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。

1.3. 即時通知客戶

持牌人或註冊人應在客戶的互聯網交易帳戶內出現某些客戶活動後，立即通知有關客戶（例如透過電子郵件、短訊服務或其他推播通知）。這些活動至少應包括：

(a) 登入系統；

(b) 重設密碼；

(c) 執行交易；

(d) 向第三方帳戶轉移資金（除非該等帳戶在資金轉移前已就轉移資金目的向該持牌人或註冊人進行登記）；及

(e) 更改客戶和帳戶的相關資料。

向客戶發出通知的途徑，應與登入系統時所使用者不同（如第 1.1 段所述）。

客戶只可選擇不收取“執行交易”的通知。在此情況下，持牌人或註冊人應向客戶作出充分的風險披露，及客戶應簽立一份聲明，以確認其明白不收取有關通知所涉及的風險。

1.4. 數據加密

持牌人或註冊人應以強效的加密程式：

(a) 將敏感資料，例如客戶登入資料（即使用者名稱和密碼）及交易數據，在內部網絡與客戶裝置之間傳輸時加密；及

(b) 保護儲存於其互聯網交易系統的客戶登入密碼。

1.5. 保護客戶的登入密碼

持牌人或註冊人應訂立並實施有效的政策及程序，以確保在啟動帳戶及重設密碼的過程中，客戶的登入密碼是在安全的環境下產生及發送給客戶的。客戶的登入密碼應由系統隨機產生，及透過不受人為干預及不會被持牌人或註冊人的職員竄改的溝通途徑發送給客戶。

若客戶的登入密碼並非由系統隨機產生，持牌人或註冊人應實施足夠的保安監控措施以作彌補，例如強制客戶在啟動帳戶後首次登入時更改密碼。

1.6. 嚴格的密碼政策及網頁超時監控措施

持牌人或註冊人應在其互聯網交易系統內設立嚴格的密碼政策及網頁超時監控措施，包括：

(a) 最短的密碼長度；

(b) 向長期未更改密碼的客戶發出定期提示；

(c) 最低的密碼複雜程度（即同時包含字母與數字），及重用舊密碼前須更改密碼的次數；

(d) 針對無效的登入嘗試採取適當的監控措施；及

(e) 網頁在閒置一段時間後被設定為已超時。

2. 基礎設施保安管理

2.1. 配置安全的網絡基礎設施

持牌人或註冊人應透過妥善的網絡隔離措施（即設有多重防火牆的隔離區）來配置安全的網絡基礎設施，以保護關鍵系統（例如互聯網交易系統及交收系統）及客戶數據免受網絡攻擊。

2.2. 使用者接達管理

持牌人或註冊人應設有政策及程序，以確保只容許有需要的人士接達或使用系統。此外，持牌人或註冊人應至少每年檢視使用者有權接達的關鍵系統（例如互聯網交易系統及交收系統）及數據庫（例如客戶數據）的列表，以確保只有獲核准且有需要的人士方可接達或使用系統。

2.3. 遙距連接的保安監控措施

持牌人或註冊人應只容許有需要的人士遙距接達其內部網絡，並對遙距接達實施保安監控措施。

2.4. 修補管理

持牌人或註冊人應及時監察和評估軟件提供者發布的保安修補程式或修正程式，並視乎對影響進行的評估，在切實可行的情況下盡快進行測試，並在測試完成後一個月內執行該等程式。

2.5. 端點保護

持牌人或註冊人應及時執行和更新防毒及抗惡意軟件解決方案（包括相應的定義檔案及辨識檔案），以偵測關鍵系統伺服器及工作站內的惡意應用程式及惡意軟件。

2.6. 在未經授權的情況下安裝硬件及軟件

持牌人或註冊人應實施保安監控措施，以防止硬件及軟件在未經授權的情況下被安裝。

2.7. 實體保安

持牌人或註冊人應訂立實體保安政策及程序，以確保關鍵系統組件（例如系統伺服器及網絡裝置）處於安全的環境下，及防止有人在未經授權的情況下實際接觸寄存互聯網交易系統及關鍵系統組件的設施。

2.8. 系統及數據備份

持牌人或註冊人應至少每天將其業務紀錄、客戶及交易數據庫、伺服器及證明文件在離線媒體進行備份。

持牌人或註冊人亦應採納適當的恢復方法，使重大系統變更得以成功還原。

2.9. 網絡保安情境的應變計劃

為確保在網絡保安事故發生時可有效執行適當的應變程序，持牌人或註冊人應盡一切合理努力，使其業務延續計劃及危機管理程序涵蓋可能出現的網絡攻擊情境（例如分散式阻斷服務攻擊[2]），及業務紀錄和客戶數據因網絡攻擊（例如勒索軟件）而完全損毀的情況。

2.10. 涵蓋互聯網交易的第三方服務提供者管理

若持牌人或註冊人安排將任何與其互聯網交易有關的活動外判給第三方服務提供者，持牌人或註冊人應與有關服務提供者訂立正式的服務協議，當中須訂明服務條款及提供者的責任。尤其是，持牌人或註冊人應確保第三方服務提供者所提供的服務，可使持牌人或註冊人遵守（除其他規定條文外）《操守準則》第18段和附表7以及本指引所載的相關規定。服務協議應定期予以審視，並在適當時作出修改，以反映外判安排的任何變更或監管發展。在可行的情況下，有關協議應以量化方式詳細規定服務提供者需提供的足夠保養及技術協助。

3. 網絡保安管理及監督

3.1. 網絡保安管理層的角色及責任

負責互聯網交易系統的整體管理及監督的負責人員或主管人員，應設定網絡保安風險管理框架（包括但不限於政策及程序），及列明主要角色及責任。這些責任包括：

(a) 審視及批准網絡保安風險管理政策及程序；

(b) 審視及批准有關網絡保安風險管理資源的預算及開支；

(c) 安排定期就整體網絡保安風險管理框架進行自我評估；

(d) 審視透過網絡保安事故報告機制上報的重大事件；

(e) 審視內部和外部稽查及網絡保安檢視所識別出的重大發現；批准作出補救行動及監察有關工作直至行動完成為止；

(f) 監察及評估最新的網絡保安威脅及攻擊；

(g) 審視及批准業務延續計劃，當中涵蓋網絡保安情境，及為互聯網交易系統而設立的相關應變策略；及

[2] 分散式阻斷服務攻擊指多個受操控的電腦系統一同攻擊某個伺服器、網站或其他網絡資源，導致攻擊目標的用戶被截斷服務。

(h) 審視及批准與互聯網交易有關的第三方服務提供者的服務協議及合約（如適用）。

這些責任可以書面形式轉授予指定委員會或營運單位，但整體責任仍由負責人員或主管人員承擔。

3.2. 網絡保安事故報告

持牌人或註冊人應訂立書面政策及程序，訂明懷疑或確實的網絡保安事故應以何種方式上報及向內（例如負責互聯網交易的負責人員或主管人員）和向外（例如客戶、證監會及其他執法機構（如適用））報告。

3.3. 內部系統使用者的網絡保安意識培訓

持牌人或註冊人應至少每年向所有內部系統使用者[3]提供足夠的網絡保安意識培訓。在設計培訓課程的內容時，持牌或註冊人應顧及其所面對的網絡保安風險類別及水平。

3.4. 向客戶發出網絡保安警示及提示

持牌人或註冊人應採取一切合理步驟，就網絡保安風險及有關使用互聯網交易系統的建議預防和保護措施向客戶發出提示及警示，例如登入資料應妥為保管及不能共用。

[3] 內部系統使用者指任何可接達持牌人或註冊人的內部網絡和系統的常額職員及合約職員。