網絡保安

本常見問題旨在就實施《降低及紓減與互聯網交易相關的黑客入侵風險指引》（《指引》）提供更多指導，並輔以實例說明。

1.1 雙重認證

問1: 互聯網經紀行在選擇雙重認證解決方案時，應考慮甚麼因素？

答: 雙重認證是一項以原則為本的認證規定。互聯網經紀行可自由選擇與其安全基礎設施最為匹配、並適合用來實現其風險紓減目標的雙重認證解決方案（包括內部研發的解決方案）。

尤其是，互聯網經紀行應評估及衡量不同雙重認證解決方案的特點、局限性和漏洞，並按情況所需制訂監控措施以作彌補。如有需要，應尋求解決方案提供者或技術顧問的協助。舉例來說，互聯網經紀行如使用短訊傳送一次性密碼，便應告誡其客戶不要設定短訊轉發。

隨著時間過去，某些雙重認證解決方案可能會因科技進步而變得不合時宜及無效，因此，互聯網經紀行應盡其合理努力緊貼最新的科技發展，並完善其雙重認證解決方案，或在有需要時採取補足監控措施。

問2: 可否採用"雙重密碼"模式（例如在登入系統時使用一組密碼，而在落盤時則須輸入另一組密碼；或在登入系統時須輸入兩組不同密碼）來符合雙重認證規定？

答: 否。雙重密碼只構成認證程序中的單一因素（即"客戶所知的"），故不符合雙重認證規定。

1.2 實施監察及監督機制

問3: 可否舉例說明互聯網經紀行可如何偵測未經授權而接達客戶的互聯網交易帳戶的情況？

答: 互聯網經紀行可監察是否有下列情況：(i) 由同一個IP地址登入多個客戶帳戶；及(ii) 接達同一個客戶帳戶的IP地址在短時間內由一個國家轉為另一個國家。

1.3 即時通知客戶

問4: 如客戶已就不尋常的登入情況（例如，並非透過客戶慣常使用的裝置登入）收到通知，互聯網經紀行是否仍須就每次系統登入通知客戶？

答: 本會要求互聯網經紀行須就每次系統登入即時通知有關客戶。然而，只要符合以下規定，互聯網經紀行可以讓客戶選擇不就每次系統登入收取通知：

- 互聯網經紀行有能力識別不尋常登入及就不尋常登入即時通知客戶；
- 互聯網經紀行向客戶作出了充分的風險披露，而客戶已確認他們了解選擇不就每次系統登入收取通知所涉及的風險；及
- 客戶沒有選擇不收取執行交易的通知。

1.4 數據加密

問5: 就數據加密規定而言，隔離區是否被視為內部網絡的一部分？

答: 是。就上述規定而言，隔離區會被視為內部網絡的一部分。

1.6 嚴格的密碼政策及網頁超時監控措施

問6: 互聯網經紀行應每隔多久，便要提醒客戶更改密碼？

答: 我們一般預期，如客戶超過90個曆日未有更改密碼，互聯網經紀行便應提醒有關客戶更改密碼。

問7: 互聯網經紀行可對多次嘗試登入無效的情況採取甚麼監控措施？

答: 互聯網經紀行可採取的監控措施包括：

- 封鎖帳戶；
- 連續登入失敗的情況每發生一次，暫停登入的時間便會延長；及
- 偵測是否受到暴力破解攻擊，並採取適當的對策。

以上所列的監控措施並非詳盡無遺。互聯網經紀行可選擇採取任何其認為適當的監控措施。

2.8 系統及數據備份

問8: 是否可將"遙距備份伺服器"視為用於系統及數據備份的"離線媒體"？

答: 是。"離線媒體"[1] 一詞是指與生產系統安全隔離的磁帶或任何其他類型的媒體（例如遙距備份伺服器）。

[1] 請參閱《指引》第2.8段及《證券及期貨事務監察委員會持牌人或註冊人操守準則》附表7第1.2.6(b)段