

香港：證監會通函虛擬資產交易平台說明保管要求（8/15）

香港證監會對所有持有虛擬資產交易平台執照業者發出通函，說明對於穩健保管客戶虛擬資產的要求，由於海外的中心化虛擬資產平台在過去一年發生多起網路安全事件，引發重大財務損失，各項事件凸顯重大漏洞^{註1}，顯示虛擬資產交易平台應檢視並加強資產保管措施，通函重點摘要如下：

■ 高階管理階層職責

- 高階管理階層應落實有效政策、程序和內部監控措施，並指定至少一名負責人員，確保平台有效運用資源及程序，進行營運活動。

■ 客戶冷錢包的基礎設施

- 平台營運者採用硬體安全模組(Hardware Security Module, HSM)^{註2}供應商前，應做出適當的盡職調查及定期評估。
- 平台營運者應確保供應商有能力並持續承諾進行以下事項：
 - ✓ 有效的修正、管理以維持資安標準；
 - ✓ 在需要修正以維持硬體安全模組的資安標準時，可確保維修後硬體安全模組獲得並即時更新認證。
- 冷錢包的實施不應包含公鏈上的智能合約，減少與鏈上智能合約相關的潛在網路攻擊。

■ 客戶冷錢包之操作

- 加密種子^{註3}或私鑰之產生及保護應在與網路隔離的冷錢包設備上進行。
- 平台營運者應實施穩健且有系統的監控措施，以防止冷錢包進行未經授權的交易，且應採用白名單監控措施。

- 用於核准交易的設備應屬專用性質，其功能及網路連接均須受到限制，並與通用工作設備隔離，降低遭入侵的風險。

■ 使用錢包解決方案及第三方服務提供者

- 平台營運者必須對錢包系統程式碼(不論內外部開發)管理，嚴格執行職責劃分及監管機制。監管機制包含程式碼審查、測試、軟體供應鏈管理、管理階層的核准及安全部署手段等把關程序，降低外部攻擊者或惡意第三方開發者植入惡意程式碼的風險。
- 第三方評估應包含獨立的程式碼審查。在建立業務關係或實施重大變更前，了解提供者的軟體開發和發布流程。
- 平台營運者應就處理緊急情況和業務延續計畫的情境制訂程序，並進行演練。

■ 持續進行即時威脅監控

- 平台營運者應將鏈上客戶資產與分類帳餘額進行即時對帳。如任何非預期交易導致差異，平台營運者應立即通知資安營運中心或具備同等職能的監管團隊，採取適當的措施。
- 平台營運者應建立穩健機制，偵測未經授權而存取或入侵關鍵錢包基礎設施的情況，當中包括冷錢包保管庫、簽署設備、資料庫、生產環境軟體及程式碼儲存庫。
- 平台營運者應全天候(包含假日)進行資安監控及配置充分資源因應突發狀況。

■ 培訓與意識

- 平台營運者尤其應確保交易簽署人接受全面培訓，充分了解驗證規定，以及在交易出現任何例外或不確定情況時的適當處理程序。
- 平台營運者應採取穩健的措施，以防止盲目簽署的情況，並確保有效地以手動方式審查或核准交易。

註 1：重大漏洞包含：

- 1.攻擊者透過植入惡意程式碼，破壞第三方錢包，竄改平台的用戶界面。
- 2.存取控制措施不足，導致攻擊者可在未經授權下連結已授權設備並進行惡意更改。
- 3.系統及獨立交易的驗證不足，未能阻止交易簽署人以手動方式核准詐欺性交易。
- 4.交易簽署人在未核對內容的情況下，盲目核准虛假交易。

註 2：用以保護及儲存加密金鑰，並防止竄改之實體設備。

註 3：用以生成私鑰之隨機生成序列，作為用戶如於裝置遺失等突發狀況時，可用於回復錢包及數位資產。

資料來源：[香港證監會](#)