

資通安全宣導

臺灣證券交易所
券商輔導部

委外廠商管理不當

事件原因：證券商對測試系統與正式系統未隔離，並提供廠商高權限帳號及遠端登入功能，廠商於盤中進行系統下單測試。

影響範圍：造成1.4億元鉅額錯帳，回補後虧損113萬。

處理措施：落實網段區隔及加強上線管控作業。

對帳單郵件寄送異常

事件原因：證券商對帳單系統，因使用預設例外處理，致郵件組成後送錯收件者。

影響範圍：造成部分個人資料外流。

處理措施：確保外送郵件內容正確，程式撰寫應避免錯誤強制略過。

對外服務系統遭受攻擊

事件原因：證券商員工認股系統遭受攻擊，駭客取得相關主機帳密後，橫向移轉至重要系統，並嘗試外傳資料。

影響範圍：部分主機遭安裝惡意程式。

處理措施：立刻斷網，請外部資安公司協助。

近期案例介紹

資訊廠商「行情報價系統」異常

事件原因：因當天開盤爆量，行情傳輸需求爆增，造成報價主機資源滿載，報價服務異常，影響使用該報價資訊之證券商APP服務。

影響範圍：共4間證券商受影響，投資人無法取得行情報價，影響時間為09:05~09:35，共30分鐘。

處理措施：資訊廠商緊急增加報價服務機組數量，逐漸恢復服務，後續排定報價主機升級計畫、汰換設備。

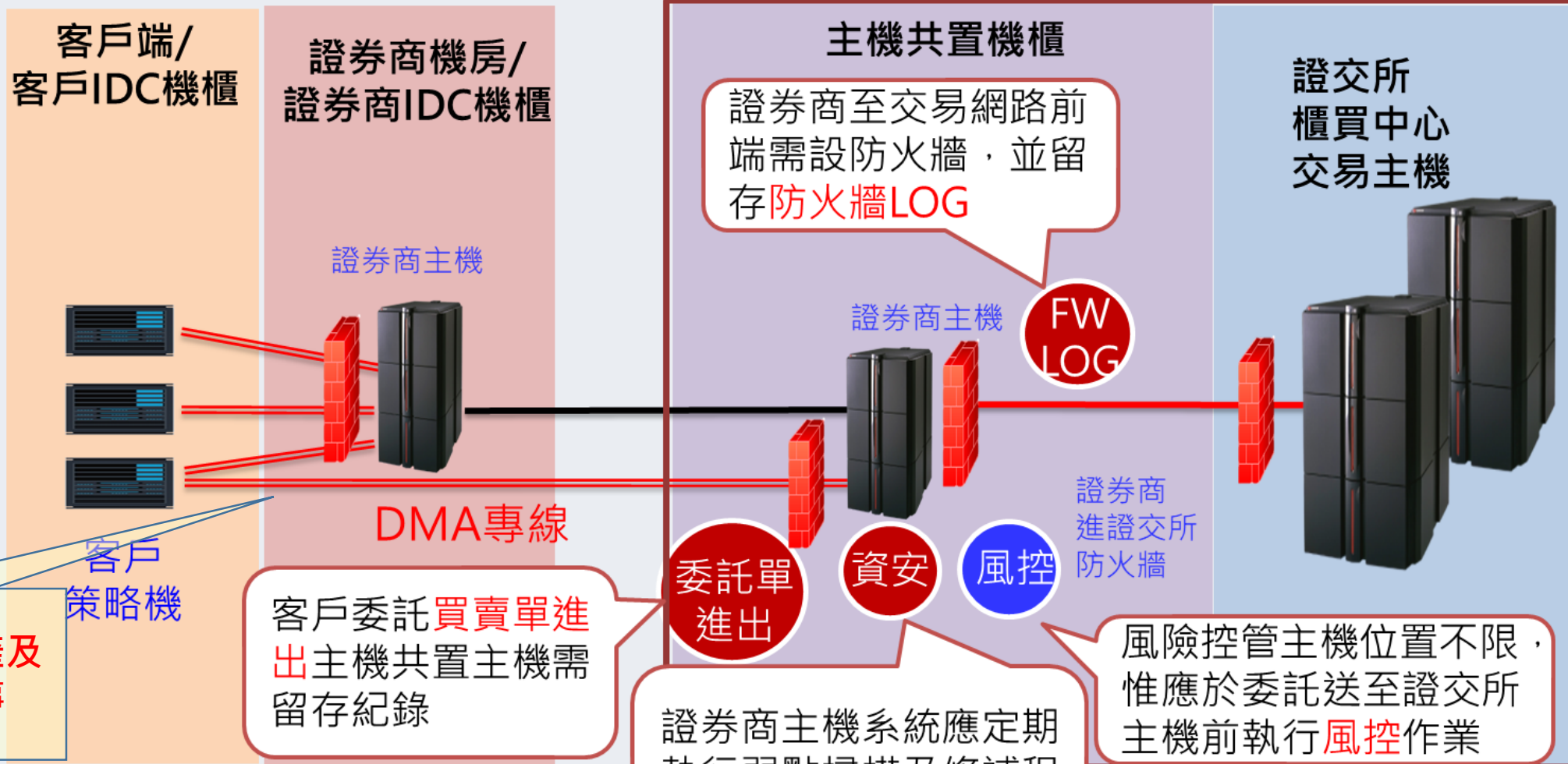
對外網站遭撞庫攻擊

事件原因：某證券商日內發生3次撞庫情事，惟有建置雙因子登入機制而未受損。

影響範圍：雖未遭撞庫成功，仍有部分客戶帳號遭鎖定

處理措施：對外網站應建置防止自動化登入機制

證券商就上述項目，應訂有內稽內控制度並留存稽核軌跡



主機共置服務

不可有放置非公司資產及替客戶保管設備之情事

客戶委託買賣單進出主機共置主機需留存紀錄

證券商主機系統應定期執行弱點掃描及修補程式安裝並留存資安紀錄

風險控管主機位置不限，惟應於委託送至證交所主機前執行風控作業

落實資安通報

- 符合資安通報態樣者應依規定進行通報。

遵守法規要求

- 不可有放置非公司資產及替客戶保管設備之情事

強化個資管理

- 強化管控個資處理流程，確保個資不外流

別讓供應商成為豬隊友

資料外洩一次；一輩子不再信任

一個小洞，沉了一艘大船