【資安事件 狀況說明】

1. 本公司於 2023 年 6 月 29 日上午, 發現公司內部特定測試環境中, 遭受外部團體之網路攻擊, 並擷取相關資訊. 當日我們即與客戶完成通報並致歉, 同時即邀請第三方資安團隊與客戶共同做損害控管.
2. 遭受攻擊之環境為工程測試區, 此為替客戶準備之系統安裝環境, 遭擷取之內容為安裝設定檔等參數資訊, 但因使用到特定客戶之公司名稱, 故引起網攻團體之注意, 並試圖經此途徑取得客戶之機敏資料.
3. 因上述資訊並無關客戶之實際應用, 僅為出貨時之基本設定, 目前沒有造成客戶之損害, 客戶也並未因此遭駭.
4. 公司已關閉受感染區段, 第三方資安團隊目前也評定其餘網段環境為正常未受損, 同時持續協助我們釐清風險足跡, 檢討改善強化資安措施.
5. 公司營運狀況一切正常, 並無造成公司實質損失, 目前也同時完成調查局的立案, 已進入刑事調查階段.
6. 原因檢討與改善:
   本次事件肇因於 a. 測試區環境防火牆版本未即時更新
   b. 測試區密碼強度不足
   c. 區內之客戶名稱未作適當的遮蔽

   本公司除已檢討並補正外, 亦同時規畫調整資安規範與網路架構, 確保內部環境資訊安全與即時監控, 以因應更為進化的資安攻擊型態.

擎昊科技股份有限公司
2023.7.4