Cyberview
力悅資訊

只要10分鐘！力悅帶你從金融資安裁罰案，看懂法遵要求！

根據iThome 2021資安大調查，重視資安的金融業，未來面對駭客攻擊、透過社交工程手法發動攻擊、勒索軟體，以及資安漏洞事件的四大資安威脅風險，成為金融業強化資安防護的首要課題。

金管會於109年8月6日推動『強化金融資安行動方案』，旨在提供民眾安心便利、穩定不中斷的金融服務，從強化主管機關資安監理、深化金融機構資安治理、精實金融機構資安作業韌性、發揮資安聯防功能四大面向切入，加強檢查金融業的資訊安全措施。

以今年上半年為例，金管會針對多家金融業有未落實資訊安全作業及未確實執行內控等缺失進行裁罰，歸納以下資安缺失：（參考資料來源：金融監督管理委員會）

1 主機未落實帳號密碼控管

(1) 主機使用者密碼未設定有效期限、與前三代重複、密碼長度不符合規範。
(2) 資料庫之使用者帳號有未說明權限及用途。

2 遠端連線未符合安全機制

(1) 未能妥適控管委外資訊廠商遠端連線至內部主機。
(2) 遠端連線驗證機制欠嚴謹，未採取OTP方式驗證，不利防範帳號遭盜用之異常情事。
(3) 遠端連線監控機制欠完整，未監控非上班時間登入等異常連線行為。

3 網頁程式與檔案未建立監控機制

(1) 對已發現之網頁錯誤訊息未妥善處理。
(2) 網路系統資安防護未能有效阻擋攻擊事件，不利網路安全與攻擊防護。

力悅資訊為「資安領域領導品牌」，集結人員、流程及技術領域數十年的經驗與專業知識，借鑒成功導入各產業客戶經驗，運用以下方案助力金融業降低資安風險，以滿足資訊治理與遵循法遵與法規要求。

金融業資安防護最佳解決方案

裁罰議題	力悅解決方案	功能簡述
主機未落實帳號密碼控管	CYBERARK PAM	**建立零常設特權安全存取** CYBERARK PAM提供整合式入口網站對納管設備/服務等進行帳號集中控管、存取控管、行為監控及操作稽核等管理作業，降低違規使用特殊權限帳號，以及駭客入侵而造成的資安事件。
遠端連線未符合安全機制	CYBERARK PAM + VPAM + MFA	**建立零信任網路安全防禦** 委外廠商自外部網路連入內部系統進行維運時，避免在遠端連線設備上輸入帳密(尤其是特權帳密)。透過CYBERARK VPAM登入平台以個人帳號進行多因子身分驗證，並採行更加嚴謹的「生物識別驗證機制」，確保遠端連入時的驗證，建立外網連線的TERMINAL GATEWAY，完整留存系統維運時的操作記錄與影像擷取，作為日後稽核與備查。
網頁程式與檔案未建立監控機制	CYBERARK SWS + EPM + BITDEFENDER EDR	**建立零威脅終端安全防護** CYBERARK SWS + EPM解決方案 • 為終端裝置實行最小特權存取，保護及更換本地管理員密碼，防堵憑證竊盜，增強安全性。 • 禁止限制用戶安裝操作未經批准/未知應的應用程式或網頁，記錄用戶在受保護應用程序中採取的操作行為，以防止企業資產或機密資料被存取。 • 防禦、阻止及遏制終端上的惡意程式及攻擊，以防止橫向移動及惡意軟體傳播，從而降低風險。 同時搭配BITDEFENDER EDR保護企業內所有內部網路的端點包括用戶設備、虛擬/實體基礎設施，以中央化的管控與防護，主動式偵測病毒、間諜程式、垃圾郵件、網路釣魚與其他惡意程式攻擊，強化企業的效率且降低管理費用與惡意程式威脅的風險，全面提升企業資安防護力。

[撰文者：力悅資訊 李曉蕾]

更多方案內容，請參閱以下官方資訊：

力悅資訊官方網站 http://www.cyberview.com.tw/cyberark

力悅資安頻道 https://www.youtube.com/channel/UCFpYkj6GaEnGoTNslRf9oUg

力悅資訊粉絲專頁 https://www.facebook.com/Cyberview2005/