政府機關資通安全防護精進建議

112 年 8 月

為強化我國資通安全防護及降低資通安全風險，賡續推動資通安全管理法及各項資通安全政策，基此，本署彙整近期資安攻防演練常見缺失及資安威脅態樣之防護建議供各機關參考，請各機關應持續加強監控即時應處，以全面提升資安防護量能。

一、 **112 年上半年**攻防演練常見缺失如下，請確實檢查並予以補強

(一) 使用者帳號密碼被取得，例如：

1. 使用預設帳號密碼。
2. 帳密或帳密規則揭露於網站、文件或影片等。
3. 弱密碼(帳號密碼相同或密碼複雜度≦2 種組合)。

(二) 資料庫(敏感性資料如密碼或個資)未採取加密儲存或遮罩等保護措施。

(三) 發現注入攻擊弱點類型，如 SQL Injection、Cross-Site Scripting 等。

二、近期資安威脅態樣之防護建議

（一） 近期發生勒索病毒跨機關擴散問題，請各機關應全面檢視與自身有網路連線之機關，應確實規劃網路區隔，降低類此情形發生風險。

（二） IOT 設備應妥善規劃納入資安防護監控範圍，避免暴露於外網。

（三） 新建帳號第 1 次以預設密碼登入資通系統時，應有強制變更密碼機制，各帳號之預設密碼不宜相同，另建議提高其預設密碼複雜度。

（四） 資通訊系統之通行碼驗證機制，應避免採用易遭推論方式(如統編、流水號等)進行驗證。

（五） 各機關應持續關注資通訊設備(含網通設備)漏洞修補更新訊息，並定期進行漏洞修補，若有停止更新或支援之產品應進行汰換或加強資安防護。

三、其他注意事項

（一）資安事件不限駭侵與否、不限3級以上事件、不限核心系統，皆應依資安法進行資安事件通報。

（二）資安事件通報應由案關系統維運機關辦理(而非使用機關)，並進行後續應變復原及持續精進作業。