(ANA事件單通知:TACERT-ANA-2023032401034747)(【資安訊息】112/3/25至112/4/9執行112年3月重要活動期間警戒專案，敬請各單位協助加強資安防護作業)

1 封郵件

service <service@cert.tanet.edu.tw>
收件者: service@cert.tanet.edu.tw

2023年3月24日 下午4:30

教育機構ANA通報平台

發佈編號	TACERT-ANA-2023032401034747	發佈時間	2023-03-24 16:24:00
事故類型	ANA-資安訊息	發現時間	2023-03-24 16:24:00
影響等級	低		

[主旨說明:]【資安訊息】112/3/25至112/4/9執行112年3月重要活動期間警戒專案，敬請各單位協助加強資安防護作業

[內容說明:]

轉發 國家資通安全研究院將於 112/3/25 零時起至 112/4/9 二十四時止執行112年3月重要活動期間警戒專案，提供全天候資安服務與必要性之技術支援，以加強防護政府機關資通安全。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告及轉發。

[影響平台:]

無

[建議措施:]

本次警戒專案執行期間，敬請各單位配合下列事項：

1.請單位資安人員確認「教育機構資安通報平台」上所登錄之聯絡資料是否正確，並請保持聯繫管道暢通，如有發生任何資安事件，請立即至教育機構資安通報平台(https://info.cert.tanet.edu.tw/) 進行通報。

2.請單位加強資通安全防護措施:

(1)確認作業系統、防毒軟體，及應用程式(如Adobe Flash Player與Java等)更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。

(2)清查重要資料，並參考下列做法定期進行備份作業：

■ 定期執行重要的資料備份。

■ 備份資料應有適當的實體及環境保護。

■ 應定期測試備份資料，以確保備份資料之可用性。

■ 資料的保存時間與檔案永久保存的需求，應由資料擁有者研提。

■ 重要機密的資料備份，應使用加密方式來保護。

(3)檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要使用存取。

(4)若使用隨身碟傳輸資料，應先檢查隨身碟是否感染病毒或惡意程式。

(5)若出現異常連線警示或疑似遭受惡意程式感染時，建議立即切斷網路，避免災情擴大，並保留相關日誌以利調查

事件發生原因。

(6)加強教育訓練，請使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結，以防被植入後門程式。

[參考資料:]
(1)臺灣學術網路個資外洩事件之預防與應變指南 https://portal.cert.tanet.edu.tw/docs/pdf/20210625040615154745613883863 74.pdf
(2)IoT設備資安防護指南https://portal.cert.tanet.edu.tw/docs/pdf/20221104041140407198627396083 09.pdf
(3)網路安全管理指南 https://portal.cert.tanet.edu.tw/docs/pdf/20220905090953534173170357076 18.pdf

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw