新北市忠義國民小學網路攻擊行為與網路頻寬管理之處理機制

九十九年九月二十八日資訊教育委員會開會討論

一、本校目前阻擋網路攻擊行為與網路頻寬管理之措施如下：

1.硬體防火牆（ 友旺 FW-100 防火牆 ）阻擋規則

2.硬體防火牆（ I-chip 晶片式伺服器 ）阻擋規則

二、廣告信通報資料來源及中毒主機之偵測系統：

1.教育部電算中心網路封包偵測系統
(http://netflow.edu.tw/)

2.教網流量分析主機病毒偵測系統
(http://163.20.1.1/traffic/safe-tl.htm)

3.上層管理單位或其他 user 反映網路攻擊事件之通報

4.本校自行建置之網路攻擊偵測系統

三、中毒主機及網路頻寬不當使用主機之處理步驟：

步驟 1.先將該主機之網路線拔除或設定 router （ switch 、 firewall ）之 ACL 以限制其進出校園網路。

步驟 2.接著查明是校內正常服務之伺服器主機(server)，還是一般使用者的電腦(一般 pc)。

如果是伺服器主機(server)，其處理方式如下：

(1) 查明是否中毒或是系統漏洞問題-----儘速安裝防毒軟體和安裝修補程式

(2) 查明是否系統遭到入侵-----查明是否伺服器主機內的帳號密碼被盜用

如果是一般使用者電腦，其處理方式如下：

(1) 查明是否中毒或是系統漏洞問題-----儘速安裝防毒軟體和安裝修補程式

(2) 查明是否系統遭到入侵-----查明是否一般使用者電腦的帳號密碼被盜用

四、後續處理及回報：

1. 處理過程中，若有困難或疑問，請求教網中心網路組協助處理。
2. 若有老師自行架站者，先行口頭溝通，以道德勸說；如是惡意架站則依「校園網路使用規範」處理。
3. 完成後，插回網路線或解除校內限制，並連絡市網中心網路組協助測試。
4. 測試完成後，將發生經過與處理情形通報本校行政主管。
5. 若遭到上一層網管人員限制進出 TANet ，通報該上級單位處理結果，以便解除限制。

五、本辦法經校長核准後實施，修改亦同。