三八、國立苗栗高級商業職業學校網路攻擊行為處理作業程序

103年3月10日行政會議訂定通過

一、通報資料來源：

1.教育部電算中心網路封包偵測系統

2.教網流量分析主機病毒偵測系統

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

二、處理方式：

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

2.查明是校內正常服務之主機，還是一般使用者的電腦。

服務主機之處理方式：

1.查明是否中毒

2.修補系統漏洞

3.查明是否遭到入侵

4.查明是否主機內帳號密碼被盜用

一般電腦之處理方式：

1.查明是否中毒

2.修補系統漏洞

3.查明是否遭到入侵

三、後續處理及回報：

1.處理過程中，若有困難或疑問，請求區網中心網路組協助處理。

2.若有惡意架站者，送「校務行政電腦化管理委員會」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，並連絡區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。

四、本作業程序經行政會議通過後實施，修正時亦同。