公務機密維護宣導--【教師介聘電腦駭客案件實例研析】

一、前言

現今科技的發明，使得人們藉由無遠弗界的網路在瞬間即可跨越距離的界限，輕易到達世界上的任何一個地方，也正因如此，掌握資訊的流通及作好訊息的防護已成為本世紀資訊戰中最要的一個課題。正因為網路的特性，使得防制滲透及機密維護扮演著國家安全、機關安定中最重要的角色。近來，有些公務機關發生遭駭客入侵滲透竊取機密或竄改資料甚至癱患系統之情形，例如單純的教師介聘作業亦遭有心人士入侵竄改，顯示對於防制滲透與機密維護之觀念有待加強，因此本文僅就該案例作一探討，由實務中加強正確觀念，以求電腦駭客案件能有所減少。

二、案例介紹

（一）緣由：

教育部自民國 90 年起為辦理臺閩地區公立國中小學暨幼稚園教師申請介聘他縣市服務之作業，依「90 年臺閩地區公立國民中小學暨幼稚園教師申請介聘他縣市服務作業要點」實施相關聯合介聘作業，並以電腦作業方式行之，由教育部委託○○縣電子資料中心負責辦理相關流程。欲申請調動外縣市介聘之教師則於填寫介聘申請表後，上網至該中心所架設之「教師外

縣市介聘網站」登錄資料。

（二）案情概述：

本案係 94 年5 月間某國小沈姓資訊組長因其甲教師友人欲請調回臺北縣服務，不諳電腦網路操作而將其個人電腦帳號、身分證字號等資料交由沈某，由沈代為操作網路程序向電子資料中心提出介聘調動申請，沈遂於5 月31 日利用學校IP 透過某大學的代理伺服器連結，進入介聘作業系統，沈先隨意試著更改不認識的某國小乙老師的積分，以及丙老師的志願，沒想到都更改成功，便更改甲姓友人和認識的丁老師兩人積分。沈自行模擬調動兩次，發現甲與丁師無法如願調成，遂將兩人資料還原，但因已忘記乙、丙老師的資料，所以無法還原，導致兩名老師，一個積分由131 分被竄改為101 分，另一個的第一志願則被更改。由於乙老師一心一意想調回住家所在的臺北縣，因此對於介聘分發十分留意，時常上網查看自己積分，經發現積分由131 分被竄改為101 分，被介聘到其他國小，經向彰化縣教育局反映，並確認並非鍵入錯誤，轉向高縣教育局通報，才發現分發作業系統遭駭客入侵，另一名丙老師則因原本績分不足，無法調動，故不受影響。

（三）適用法條：

本案係適用《刑法》新增之第 36 章妨害電腦使用罪，其中第359 條「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」以及361 條「對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一」，由於沈○○犯後即向服務學校校長坦承，透過校長向花蓮縣教育局報告，並告知高雄縣電子資料中心，表示願主動投案，全案後由高雄縣調查站及高雄警察局調查了解，因沈某屬自首行為，且犯後坦承不諱全力配合調查，經高雄縣調查站偵訊後依違反個人資料保護法移送高雄地檢署，由檢察官諭令五萬元交保，並宣告緩起訴處分。

三、缺失檢討與應有正確觀念

（一）缺失檢討：

本案係沈某利用介聘系統網站的網頁漏洞，於進入介聘系統網站之系統管理者目錄網頁後，取得系統管理者權限入侵竄改資料之權限，係因本案與防火牆的防護機制不足有關，因辨識身分之設計無法確實把關，導致遭人入侵滲透，而高雄縣電子資料中心亦表示本案係為求方便在主辦單位新竹縣教育局的遠端連線，於作業期間取消「最高管理員程式區」的IP 限制，

造成漏洞而使有心者滲透入侵而產生，因此已要求電子資料中心在事發後緊急更改入口程式，加強阻擋駭客的入侵。因此缺乏必要的防護機制及因貪求一時之快而開方便之門都可能給予駭客入侵的最佳機會。

（二）正確的資訊維護觀念：

正確的資訊維護觀念是對付駭客入侵的重要關鍵，除了透過防毒軟體、防火牆系統等防護機制外，重要資料最好不要存放於電腦裡，並做好使用程式及瀏覽器、WORD 等應用程式和防毒軟體定期、隨時更新，以避免漏洞，並養成不隨便讀取來路不明電子郵件習慣，免得「開後門」讓駭客有可乘之機，都是正確且必要的資訊維護觀念。

四、結論

本次的教師介聘電腦系統案，雖僅有一位老師權益受影響，並於事後予以彌補，但其中所顯現的機制漏洞有關單位實應妥慎檢視省思，畢竟未來「電子政府」已是趨勢所在，如讓前述的駭客入侵案件一再發生，將嚴重損及我國家安全及機關安定。

（本文轉載自清流月刊）