資安事件案例及因應作為

教育部資訊及科技教育司

111年9月5日

大 綱

1. 8月警戒期間資安事件及後續因應
2. 大專校院重要資安政策
3. 高等教育深耕計畫資安專章
4. 大專校院資安長督導協助事項

1. 8月警戒期間資安事件及後續因應

1.1 警戒緣由
1.2 迅速因應網頁遭竄改事件
1.3 落實管理全校物聯網設備
1.4 限制對外出租場域使用大陸廠牌資通訊產品

1.1 警戒緣由

111年8月警戒專案

- **行政院**國家資通安全會報技術服務中心**接獲外部情資**，**8月**可能有**大規模網路攻擊**行為。
- 於111年**8月期間**成立資安警戒專案，請各機關加強資安維運暨系統之防護。

111年8月網軍攻擊

- 受近期**國際政經情勢影響**，除中國於臺海展開軍演，我國亦遭受外國網軍**組織性攻擊**：
  - 我國政府機關、民間企業傳出諸多災情，包含**大專校院**。
  - 主要**竄改、阻斷**我國「**具傳播力**」之資通訊系統，以對民眾發動**心理戰**。

資料來源: Youtube，網軍APT27官方頻道

8月警戒期間攻擊態樣(阻斷服務)

- **傳播媒體**、**重要網站**的服務被影響或**阻斷**

民視新聞-線上直播頻道

圖片來源： ETtoday新聞雲 111/8/3 報導，
https://www.ftvnews.com.tw/news/detail/2022803W0141

國防部、外交部-官網

圖片來源： ETtoday新聞雲 111/8/5 報導，
https://www.ettoday.net/news/20220805/2309470.htm

1.2 迅速因應網頁遭竄改事件

8月警戒期間攻擊態樣(網頁遭竄改)

- 學校/機關**對外服務網頁**被**竄改**

大學-行政單位官網

圖片來源： ETtoday新聞雲 111/8/7 報導，
https://www.ettoday.net/news/20220807/2311348.htm

高雄市政府-政策宣導網站

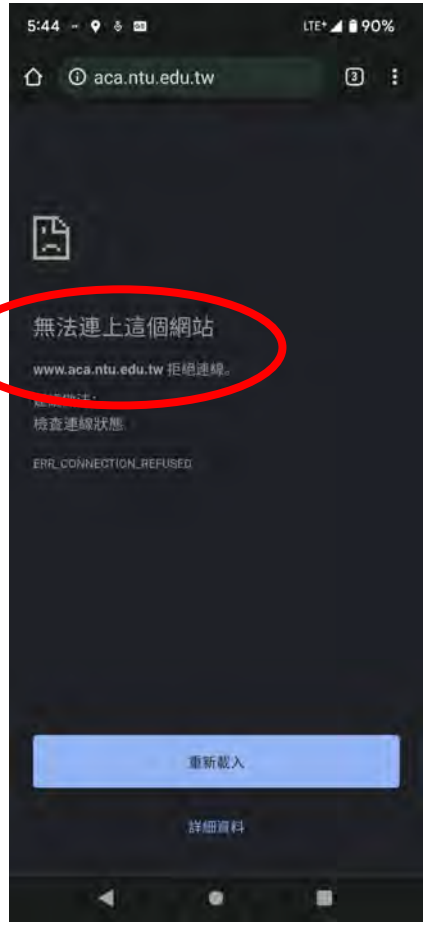
圖片來源： 聯合新聞網 111/8/4 報導，
https://udn.com/news/story/7327/6513343

網頁遭竄改緊急應變原則(1/3)

- 參考行政院111年8月資安警戒專案相關會議指示，如發現所轄管系統網站內容遭竄改，應依下列原則辦理**緊急應變**：
  1. 原網站**立刻下架**。(注意亦須完成跡證保全及留存)
  2. **維護公告**網頁：**10分鐘內上架**。
  3. **靜態資訊**網頁：網站功能**無安全疑慮**的部分可先上架**恢復服務**，如純資訊公告、媒體播放等。
  4. 逐步**功能恢復**：網站每次**版更上線前弱點掃描**，確認**無重大安全性弱點**。(必要時加入人工測試)
  5. 全面修復上架。

網頁遭竄改緊急應變原則(2/3)

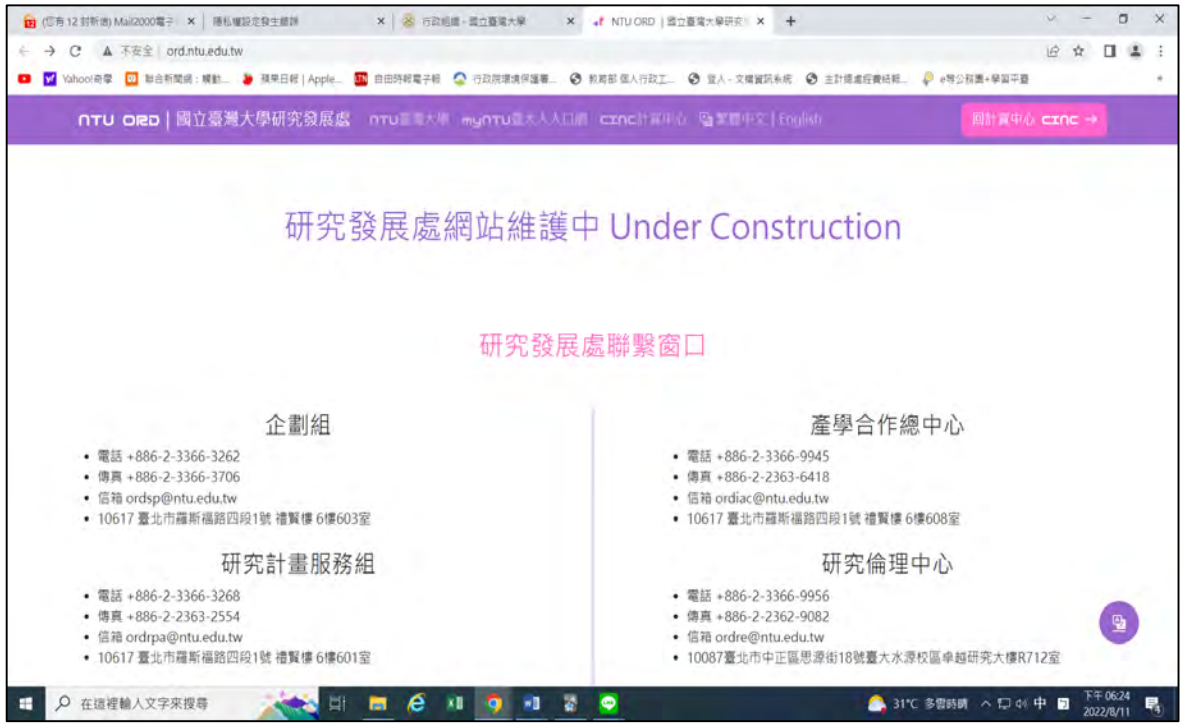
網頁內容遭竄改



原網站
立刻下架

網頁遭竄改緊急應變原則(3/3)

維護公告頁面



電腦版面

手機版面

大專校院應辦事項(網頁遭竄改)

- 依資安法及「臺灣學術網路各級學校資通安全通報應變作業程序」規定，落實**資安事件通報**及**應變**作業(於**知悉1小時內完成通報**)。
  - 訂定內部作業規範且**適用範圍為全校**(含各行政單位、系所)。
  - 實施**教育訓練**或辦理演練，使相關人員確實熟悉作業程序。
- 針對網頁**遭竄改**事件：
  - **備妥應變機制**。請各行政單位、系所**盤點所管網站**，**事先建立維護公告**頁面及**切換機制**，以利及時應變。(發現網站內容遭竄改後10分鐘內切換為維護公告頁面)
  - **「行政單位、系所網頁遭竄改」**應納入學校**業務持續運作演練(BCP)**演練情境，並請相關單位**實際演練緊急應變**作業程序。

1.3 落實管理全校物聯網設備

8月警戒期間攻擊態樣(物聯網設備入侵)

- 學校/機關、民間企業內**物聯網設備**被入侵，並取得**管理權限**。

7-ELEVEN超商-連網**電子看板**

圖片來源：民視新聞網 111/8/3 報導，
https://news.tvbs.com.tw/politics/1866977

國小-能源管理系統

物聯網設備安全風險

- 學校可能面臨的安全風險
  - ➢ 無法掌握**全校物聯網設備清單**及管理情形。
  - ➢ 設備**曝露於外網**，增加被外界發動攻擊的風險。
  - ➢ 設備**管理失當**，如使用**廠商預設帳密**、**未修補重大安全漏洞**等。




物聯網設備管理原則(1/2)

- **清查全校**物聯網設備
  - **盤點範圍**包含學校**採購**、**公務使用**之物聯網設備。
  - **設備類型**包含但不限於：**網路印表機**/**多功能事務機**、**網路攝影機**、門禁設備、環控系統、無線網路基地台(AP)/路由器、**連網電子看板**、能源管理系統(EMS)等。
  - 建立物聯網設備**管理清冊**(至少包含設備類型、廠牌型號、IP、存放地點、管理單位及用途等欄位)並**定期更新**(至少每年1次)。未納管設備建議斷網。
  - 逐步汰換老舊且無安全更新支援的設備。

物聯網設備管理原則(2/2)

- **加強**設備**連線控管**
  - ➢ 依業務需求設定適當網路存取限制。
  - ➢ 無需對外開放連線者，得以防火牆限制僅供內部連線。
- **變更**設備**預設帳密**。
  - ➢ 不得使用廠商預設帳密及弱密碼。
  - ➢ 符合機關規範之密碼複雜度要求。
- **修補**設備**重大安全漏洞**。
  - ➢ 依公告漏洞情資即時進行安全性更新。

設備未作連線控管，且未變更廠商預設帳密，可能導致嚴重後果，如教職員生敏感個資外洩。

大專校院應辦事項(物聯網設備入侵)

- 依物聯網設備管理原則，落實設備安全防護。
  - **清查全校物聯網設備**，定期更新清冊，並**確認管理權責**單位。
  - 加強設備連線控管，**不得使用廠商預設帳密**及弱密碼。
  - 即時**修補**設備**重大安全漏洞**。
- **不得使用大陸廠牌**資通訊產品，如有應立即停止與公務環境介接，並盡速完成汰換。

1.4 限制對外出租場域使用大陸廠牌資通訊產品

111年8月警戒期間網軍攻擊(對外出租場域)

- 除機關/學校本身，其**出租場域**的**物聯網設備**亦遭入侵

臺鐵車站大廳-廣告推播電子看板

圖片來源：民視新聞網 111/8/3 報導，
https://www.ftvnews.com.tw/news/detail/2022803W0141

台鐵看板出現謾罵裴洛西字眼 初判廠商網路被駭

2022/8/3 12:46（8/3 12:51 更新）

（中央社記者蔡孟妤、洪學廣、汪淑芬高雄3日電）美國聯邦眾議院議長裴洛西昨晚抵台，今天上午台鐵新左營站的廣告看板，出現詆毀裴洛西的攻擊性字眼，初步研判是廠商網路被駭。另高雄有超商看板也出現異狀，警方偵辦中。

大約上午10時，有民眾發現新左營站的一處看板，出現形容裴洛西是老巫婆的攻擊性字眼。

台鐵新左營站長劉俊哲說，這面電子廣告是租給外包廣告商，由於廠商網路並非是用台鐵內部系統網路，而是連接一般網路，因此初判是廠商網路被入侵。

圖片來源：中央社 111/8/3 報導，
https://www.cna.com.tw/news/aipl/202208030138.aspx

大陸廠牌資通訊產品禁令擴大至對外出租場域

- **行政院**111年8月資安警戒專案相關會議指示：
  - 針對**傳播影像或聲音**，供**不特定人士**直接收視或收聽之情形，皆不可使用危害國家資安產品(如大陸廠牌軟體、硬體及服務)。
  - 非屬前述傳播類型之危害國家資安產品，亦須列冊管理，控管資安風險，請各機關透過**委外契約**及**場地租借使用規定**來推動辦理。


陸資通產品禁令擴大 納公務場所

2022-08-07 04:06 聯合報／記者侯俐安、邱瓊玉、葉冠妤、盧逸峰、許維寧／台北報導

+ 台鐵

台鐵新左營站電視牆日前遭駭，稱美國眾議院議長裴洛西是「老巫婆」，行政院全面要求公務場所不得使用大陸資通產品。圖為新左營站被駭的電視牆目前停用。記者劉學聖／攝影

資料來源: 聯合新聞網 111/8/7 報導，
https://udn.com/news/story/122988/6518330

大專校院應辦事項(對外出租場域)

- 限制出租場域使用大陸廠牌資通訊產品
  - 於學校**委外契約**或**場地租借使用規定**，**明訂**不得使用危害國家資安之產品（**如大陸廠牌軟體、硬體及服務**）。
  - 針對現有委外契約，協調廠商配合辦理或**修正契約規定**。
  - 備妥應變機制，如遇駭入侵，能緊急斷電下架。

2. 大專校院重要資安政策

獎勵機制

- 學校應落實資安法要求及**本部頒布之資安作業規範**，如「國立大專校院資通安全維護作業指引」。針對資安**辦理成效優良**之學校**給予獎勵**：
  - 資安**作業事項**(如社交工程演練、資安事件通報演練)成績優良者，建請學校對相關人員**行政獎勵**。
  - 建立**全校資安成效評量**機制，並針對評鑑優良者給予獎勵。
  - 將資安辦理成效**納入**學校**獎補助衡量指標**，指標項目包含但不限於：
    - **全校導入ISMS**：指ISMS**適用範圍**，至少包含全校範圍內之**核心資通系統**、**保有個資或防護需求中等級以上之資通系統**，及其相關網路與資訊機房活動。

懲處機制

- 針對**因管理不當**導致資安事件之學校**加重處罰**
  - 發生**重大資安事件**，**且未落實**本部專案稽核之缺失**改善**者：
    - 循相關機制**提報懲處**。
    - **專案評估扣減**對該校之獎補助款。
  - **管理人員**因**設置弱密碼**而導致資安事件。
    - 本部將正式請機關評估**予以懲處**。
  - 如因管理不當導致**資安事件**，以**不遮蔽**該學校方式作為教育體系**內部案例宣導**。

非技術問題，而是管理上的怠惰

教育部110年6月29日臺教資(四)字第1100085899號函
教育部110年6月29日臺教資(四)字第1100085899A號函

國立大專校院資通安全維護作業指引(1/2)

- 本部已於110年12月30日函送**國立大專校院資通安全維護作業指引**，請各校**務必落實**辦理，包含下列事項：

資安長之配置

宜指派**主任秘書以上人員**兼任

資安推動組織

宜由**資通安全長**召集全校各單位主管或副主管組成，**每年至少召開會議1次**

資通系統盤點

盤點範圍應包含**全校各單位**

內部資安稽核

稽核範圍應包含**全校各單位**

教育部110年12月30日臺教資(四)字第1100179797號函

國立大專校院資通安全維護作業指引(2/2)

- 資安維護計畫適用範圍應**涵蓋全校**(各系、院、所**教學單位**及各**行政單位**)。

資通系統盤點

- 各校每年提交之「**資通系統資產清冊**」**至少應包含**落於**各校IP網段內**、或使用**各校網域名稱**之資通系統。

內部資安稽核

- 各校得就資通系統(保有個人資料)風險高低、教學單位特性**評估訂定推動先後順序**，**分年分階段**規劃辦理，並**明訂於**各校資通安全**維護計畫**。

教育部110年12月30日臺教資(四)字第1100179797號函

其他資安管理作業指引

各級學校使用資通系統或服務蒐集及使用個人資料注意事項

教育部110年9月8日臺教資(四)字第1100122001號函

蒐集最小化

蒐集個資**不得逾越**特定目的**必要範圍**

最小授權

檔案存取權限應採**最小權限原則**

設定檢查

使用雲端服務，應**避免允許顯示其他使用者內容**，發布前應確實檢查相關設定。

加密傳輸

網路傳輸應採用加密協定(如**HTTPS**)

加密儲存

特種個資或**敏感資料**，應以**加密方式儲存**。

資料銷毀

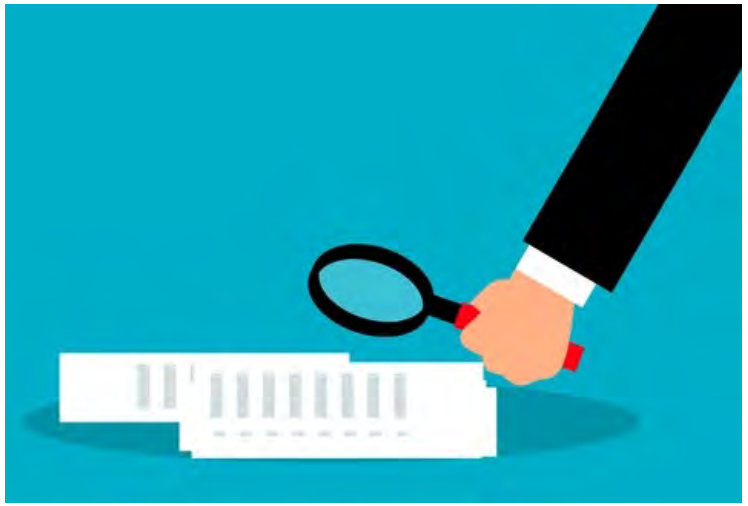
應訂個資保存期限，並於**期限或業務終止後刪除或銷毀**。

擴大教育體系資安查核輔導(1/2)

- 依資安法第13條規定，本部辦理對**國立大專校院**之**資安稽核**(包含技術檢測及**實地稽核**)，並訂定「教育部111至112年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫」。
  - 依稽核計畫，國立大專校院**稽核範圍為全校**。
  - 為強化學校**二級行政單位及系所**之**稽核強度**，本部預定於111年9月底前修正發布新版查檢項目(擬適用111年第3梯次以後受稽學校)。
  - 學校需於受稽時，由**最高管理階層**據實說明**全校性資安防護規劃**，如是否落實資安**管理制度**、資安事件**應變機制**(如針對網頁遭竄改之應變整備情形)及相關**防護措施**。

擴大教育體系資安查核輔導(2/2)

- 資安**查核輔導**範圍**擴大**至**私立大專校院**。
  - 本部將參考資通安全管理法相關規定，訂定**私立大專校院資安防護作業指引**，推動私立大專校院**逐步落實**策略面、管理面及技術面之資安要求，以提供教職員生安全的資訊作業環境。
  - 依規劃於3年內實施輔導查核作業。



大專校院應辦事項(全校性資安防護)

- 落實「國立大專校院資通安全維護作業指引」(私立大學得參照辦理)
  - **資通安全組織**由資安長召集**全校各單位主管或副主管組成**，**每年**至少**召開會議**1次。(由資安長針對重大風險事項作出處理決策，並協調各行政單位、系所配合辦理)
  - **資通系統盤點範圍**涵蓋**全校各單位**。
  - **內部資安稽核範圍**涵蓋**全校各單位**。(得依風險分年分階段辦理)
- 接受稽核時：
  - 由**最高管理階層**據實說明全校資安**管理制度**、資安事件**應變機制**及相關**防護措施**辦理情形。

3. 高等教育深耕計畫資安專章

第二期高教深耕計畫規劃說明

- 緣起
  - 本部已於107年起推動高等教育深耕計畫，協助大學發展教學創新、強化學生學習成效、善盡社會責任與發展大學特色。
  - **第二期**高等教育深耕計畫(112-116 年)將以**「專章」**引導學校提出**「資安(數位環境整備)」具體策略、措施與績效指標**，透過**審查機制**督導學校落實，並結合大數據追蹤回饋，形成發展**韌性校園**的正向循環。

第二期高教深耕計畫架構

第一部分
全面性提升大學品質及促進高教多元發展
（維護學生平等受教權）

第二部分
協助大學追求國際一流地位及發展研究中心
（強化國家國際競爭力）

第二期高教深耕計畫徵件

- 計畫徵件方式規劃
  - 俟第二期計畫奉行政院核定後，本部將另安排徵件說明會。
  - 由學校以「校」為單位，依徵件格式**提出「資安專章」計畫**，併同主冊計畫函報本部，本部將**組成專家學者審查**小組進行審查。
  - **審查完竣**後本部將**核定112年補助經費**，後續每年審查學校年度成果報告，據以核定次年度經費。

4. 大專校院資安長督導協助事項

大專校院資安長督導協助事項(1/2)

- 確認完成下列資安推動**強化作為之整備工作**：
  - **備妥網頁遭竄改應變機制**，以利於發現網頁遭竄改後10分鐘內切換為維護公告頁面，並納入**業務持續運作演練(BCP)**演練情境。
  - 落實管理全校**物聯網設備**，**全校清查**、**連線控管**、**變更預設帳密**、**修補漏洞**。
  - 透過**委外契約**或**場地租借使用規定**，要求**對外出租場域**不得使用**大陸廠牌**資通訊產品(包含軟體、硬體及服務)。
  - **強化全校性資安防護**，於接受稽核時，由**最高管理階層**據實說明全校資安**管理制度**、資安事件**應變機制**及相關**防護措施**辦理情形。

大專校院資安長督導協助事項(2/2)

- 強化資安長**領導作為**
  - ➢ **支持學校資訊單位**(如計算機中心、圖書資訊處等)管理作為，**協調各行政單位、系所遵循**其所訂定之資安管理制度及規範要求。
  - ➢ **配置**足夠**資安專責人員**，以支援全校資安整體規劃、管理及技術服務所需。
  - ➢ 因應與日俱增資安威脅，**協調**取得**所需資安經費**，如增購或汰換資安設備、翻修已過時之重要資通系統(如學籍系統)、汰換大陸廠牌資通訊產品等。

報告完畢