網站遭置換緊急應變說明

電算中心網路系統組
邱惠隆

教育部資安攻防演練通報流程

- 資安攻防演練時間:**112/11/27~112/12/29(僅上班日)**
  - 電算中心若有收到校內網站已被攻防的通知->將會寄信給已被攻防之單位SNMG成員、單位所屬一級的資安執行稽核成員、及電算中心資安小組成員
    - 敬請單位成員收到通知後盡快通知**相關網站負責人員**處理並於**48小時內處理完畢及填寫信中所附處理結果回報表單連結**，電算中心收到表單後將會確認該網站處理情形，**若無任何回覆及處理，電算中心將會先行將此網站IP斷網處理**。

教育部資安攻防演練通報流程(續)

- 建議處理方式:
  - 切換「網站維護中」公告頁面並盡快修復網站漏洞及進行弱掃。
  - 切換備援網站並將原本網站修復及進行弱掃。
  - 暫時將網站關閉。
- 如何修復:
  - 請自行逕洽該網站負責廠商修復。
  - 請單位內的網管同仁或同學協助修復。

❑ 資安攻防演練複測時間:**113/1/8-113/1/26 (針對有中高以上風險， 進行複測)**

對象

- 本說明適用對象:單位網頁伺服器主機管理人員
- 文件下載:
  - 國立中央大學資通安全專區 >政策及宣導
    - https://www.cc.ncu.edu.tw/page/isms_ncu

緊急應變原則說明

- **網站遭置換原因:**

  可能發生網頁被置換的原因是網站本身即存在漏洞，一旦被有心人士掌握，就可以在需要時隨他操弄。

  萬一不幸發生網頁被置換的情況，在手忙腳亂當下，除了緊急將網站關閉，還能夠如何處理呢？

緊急應變原則說明

- 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. 將原網站立刻下架。（建議將原本log保存）
  2. 維護公告網頁：10分鐘內發佈。
  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。
  4. 功能恢復：網站修復上線前進行弱點掃描，確認無重大安全性弱點。
  5. 完成修復上架。

網頁遭置換緊急應變處理建議(1)

❑ 網站放置於電算中心網頁空間(公務帳號)

➢ 網址為https://in.ncu.edu.tw/~ncuXXXXX(公務帳號)

單位網站若是放置於電算中心公務帳號網頁空間，當疑似因單位帳密遭竊導致網站內容被登入置換時，若無法立即將被置換網頁改回原狀，可採取以下做法：

- 密碼修改:請依照程序進行公務帳號密碼的修改。
- 置換通用版維護網頁:電算中心已事先設計通用版「網站維護中」訊息的網頁檔案，可先聯繫電算中心將單位網站首頁換成維護公告的網頁，且讓貴單位有時間將備份網頁檔還原到原網頁空間下。
- 導向備援網頁:若單位在另外的網頁空間已放置維護中訊息的網頁或重要訊息網頁，也可請聯絡電算中心將單位網站URL導向該備援網頁空間，以呈現單位客製化重要訊息，再請單位儘快修復網頁漏洞或將備份網頁檔還原到原網頁空間下。

網頁遭置換緊急應變處理建議(2-1)

❑ 單位自行架設網站

- 網址:https://xxx.ncu.edu.tw/等
- 若單位自行架設網站，建議以下作法：
  - 1.密碼修改:建議先修改主機的密碼
  - 2.事先準備另一台網站主機為備援網站，定期將網頁內容備份至此，當發生網站遭網頁置換事件或遭駭時，先將正式網站斷線後，把備份網站的IP位址改為正式網站的IP位址，讓備份網站上線。
    - 爭取時間恢復正式網站被置換的內容，也檢查網站其他功能是否也有安全疑慮並予修復。
    - 待網頁程式或主機修復後再換回正式網站主機。

網頁遭置換緊急應變處理建議(2-2)

❑ 單位自行架設網站(續)

- 3.若無額外主機可供備援，可考慮在**外部網頁空間**放置靜態網頁/維護中公告網頁或將網站首頁導至電算中心通用版「網站維護中」網頁。
  - 做法為先製作呈現單位重要資訊的靜態網頁/維護中公告網頁上傳至外部的備援網頁空間，於需要時向電算中心申請將單位網站網域名稱(DN)對應的IP位址指向外部的備援網頁空間IP，以及從原網站設定轉址。
  - 可先電話連絡修改DNS再補送申請單或寄email至DNS承辦人提供佐證，但因使用者端DNS查詢及網頁瀏覽器快取（cache）也需要時間更新，因此可能會花費較長且無法確定的時間讓臨時網站達到效果。
  - 將網站修復後記得要再聯絡電算中心DNS承辦人改回已修復的網站IP。

網頁遭置換緊急應變處理建議(2-3)

❑ 單位自行架設網站(續)

- 作法（2）單位擁有網站自主控制權，可快速讓臨時網站上線，降低網頁被置換的衝擊。
- 作法（3）單位可使用外部免費網頁空間資源提供原網站重要資訊，但生效時間無法掌握。

網頁遭置換緊急應變處理建議(3)

❑ 網站放置於電算中心二代虛擬主機服務區

- **網站IP為:140.115.197.XXX**
- 單位網站若原本建置於電算中心二代虛擬主機服務區，當發生虛擬主機遭入侵並置換網頁情況時，建議以下作法：
  - 1.密碼修改：建議修改主機的密碼
  - 2.準備外部備援網站:
    - 單位可事先在**外部網頁空間**準備「**網站維護中**」的網頁或備援網站，需要時聯繫電算中心將單位網站虛擬主機DNS指向外部備援網站。
    - **可先電話連絡修改DNS再補送申請單或寄email至DNS承辦人提供佐證，但因使用者端DNS查詢及網頁瀏覽器快取（cache）也需要時間更新，因此可能會花費較長且無法確定的時間讓臨時網站達到效果。**
    - **將網站修復後記得要再聯絡電算中心DNS承辦人改回已修復的網站IP。**

網頁遭置換緊急應變處理建議

網頁遭置換後切換維護中網頁示範

1. 自備導向語法的網頁，將首頁導向通用版「網頁維護中」網站
2. 自建「網頁維護中」網頁，且自行將首頁置換
3. 聯絡電算中心改單位DN的IP導向通用版「網頁維護中」網站

- **電算中心建置通用版「網站維護中」頁面位址:**
  - https://maintenance.ncu.edu.tw
  - 提供給需要的單位若有網站異常事件發生時，可以先自行轉址到以上位址，待網站修復後再移除轉址回復原本網頁。
- 需修改單位DN的IP時，請洽電算中心服務櫃台
  - 電話:57555、57566轉DNS承辦人
  - 劉道光先生(57508)
- **以上DNS修改說明僅限校定DNS網站(xxx.ncu.edu.tw)，若系所自己的DNS底下的網站請逕洽單位的DNS承辦人(如:XXX.mgt.ncu.edu.tw等)。**

重點提醒

- 教育部於112/11/27~12/29資安攻防演練(僅限上班日)
- 113/1/8-113/1/26 (針對有中高以上風險， 進行複測)

✓ 網頁遭置換緊急應變處理建議

網站放置於電算中心網頁空間(公務帳號)	單位自行架設網站	網站放置於電算中心二代虛擬主機服務區
• 密碼修改 • 導向"通用版"維護中訊息的網頁 • 或導向備援網頁	• 密碼修改 • 導向備援網站或靜態網頁 • 或導向"通用版"維護中訊息的網頁(也可自行建置)	• 密碼修改 • 導向備援網站或靜態網頁 • 或導向"通用版"維護中訊息的網頁(可自行建置)

請各單位依單位內網站狀況自行決定

網站基本防護作業說明

網站基本防護作業(1)

- 請各單位自行查檢項目：
  - 此檢查項目僅適用**單位自行架設網站**以及跟**電算中心申請之二代虛擬主機**
  - **存放電算中心公務帳號空間中之網站不適用。**
  - **主機:**
    - **重新檢視防火牆相關設定是否合宜**
      - 檢視主機是否有開啟未使用的網路服務協定埠，沒有使用到的網路服務協定埠請關閉。
      - **需開啟網站服務協定埠是80、443，資料庫服務協定埠3306、SSH預設22-建議改掉。(資料庫如果連到另一台主機)**
      - **限定只能存取該主機服務的IP連線(如SSH管理)。**

Linux:sudo ufw status verbose或iptables -L -n 可查看主機的防火牆規則

(請各單位可自行依單位內網頁伺服器的套件搜尋設定方法)

網站基本防護作業(2)

請各單位自行查檢項目(續)

檢視單位內測試網站與帳號等已確實關閉或移除

- 定期的檢視是否有非管理帳號存在，若有請記得移除。
- **測試帳號只有相關管理者可以使用。**
  - 帳號的確認-網頁主機伺服器: (舉例-linux主機)
- **如測試網站無法關閉，建議將測試網站限特定IP才可以連線。**

```
cat /etc/passwd 可查閱整個系統的所有帳號權限
cat /etc/group 可查閱整個系統的所有群組
```

(請各單位可自行依單位內網頁伺服器的套件搜尋設定方法)

網站基本防護作業(3)

❑ 請各單位自行查檢項目(續)

➢ 確認內部使用網站未暴露於網際網路

- 設定特定範圍的IP才能存取內部網站，可使用非特定範圍的IP連線，測試是否能連到該網站。
- **例如:限定140.115.XXX.xxx的IP可以連，可以使用手機的行動網路(非wifi)測試連到該網站，若是連不到代表此設定是有效，若連得到代表此設定是無效的，需要重新設定限制規則。**

網站基本防護作業(4)

請各單位自行查檢項目(續)

- 舉例:如何設定 nginx 阻擋特定 ip / 網段存取，首先找到對應的 nginx configuration，

```
通常會在 /etc/nginx/sites-enabled/*.conf 或是預設的 /etc/nginx/nginx.conf
      接著找到 server / location 區塊，加上 deny 語法
      server {
            listen 443 ssl http2;
            server_name xxx.edu.tw
            deny x.x.x.x # 阻擋特定 ip

      ...
      }
# 或者在指定的 location 區塊中
location / {
      # 阻擋 xxx.xxx.xx.0 ~ xxx.xxx.xx.255 的所有 ip
      deny xxx.xxx.xx.0/24;
      index index.php index.html index.htm;
      try_files $uri $uri/ /index.php?$args;
}
# 進階一點搭配 allow 的用法
server {
      listen 443 ssl http2;
      server_name blog.camel2243.com
      # 阻擋除了 ip 為 xxx.xxx.xx.235 以外的 xxx.xxx.xx.0 ~ xxx.xxx.xx.255 網段
      allow xxx.xxx.xx.235;
      deny xxx.xxx.xx.0/24;
      …(請各單位可自行依單位內網頁伺服器的套件搜尋設定方法)
}
```

網站基本防護作業(5)

- 網站基本防護作業自我檢核表(詳見檔案)

網站基本防護作業自我檢核表

檢核日期:　　年　　月　　日

單位	網站 IP 及網址	備註

項目	說明	是否確認	備註
重新檢視防火牆相關設定是否合宜 *註 1	檢視主機是否有開放未使用的網路服務埠，沒有使用到的網路服務埠請關閉。 ● 限定能存取該主機的 IP 連線。 ● 例如:網站服務埠是 80、443，資料庫服務埠 3306(資料庫如果連到另一台主機)	□未確認 □已確認	
檢視測試網站與帳號等已確實關閉或移除 *註 1	定期的檢視是否有未建立或其他的帳號存在，若有請記得移除。 ● 建議測試網站僅限特定 IP 可以連線。 ● 測試帳號只有相關管理者可以使用。	□未確認 □已確認	
確認內部使用網站未暴露於網際網路 *註 1	設定特定範圍的 IP 能存取內部網站，使用非特定範圍的 IP 連線，測試是否可以連到該網站。 ● 例如:限定 140.115.x.0/24 範圍的 IP 可以連，這樣的話可以使用手機的網路(非 wifi)測試連到該網站，若是連得到代表此設定是無效的，可能就需要重新設定限制規則。	□未確認 □已確認	
單位內是否有準備緊急應變網頁或備用網站	例如: ● 【網頁維修中】宣告頁面。 ● 備用網站	□未確認 □已確認	

*註 1:此檢查方式僅適用單位自行架設網站、及放置於電算中心虛擬主機服務區

網站基本防護作業

- 建議:
  - 定期檢視網頁主機的作業系統、網站伺服器、及網頁應用程式、套件等版本更新與漏洞修補。
  - 網站備援與定期(建議每日)備份重要資料等防護措施。
  - 應定期檢視網路、系統有無異常狀況及進行網站弱點掃描。

網站基本防護作業

結語:

本簡報僅傳達當**網頁遭置換時**的**緊急應變建議作法**，追根究底還是應該**強化網站的安全性，包含作業系統、網站伺服器、及網頁應用程式等版本更新與漏洞修補，定期進行網站弱點掃描也可提供修補改善建議**，以**防堵**因伺服器本身問題導致遭入侵而引發的網頁置換，或甚至資料外洩、遭攻陷成為傀儡跳板機等更嚴重的**資安事件**。

重點提醒

✓ 網站基本防護作業

重新檢視防火牆相關設定是否合宜	檢視單位內測試網站與帳號等已確實關閉或移除	確認內部使用網站未暴露於網際網路
• 沒有使用到的網路服務協定埠請關閉 • 限定只能存取該主機服務的IP連線	• 定期的清查帳號 • 測試帳號只有相關管理者可以使用 • 特定IP才可以連線內部測試網站	• 限制特定範圍的IP才能存取內部網站

請各單位依單位內網頁伺服器的套件及狀況自行搜尋設定方法

Thank You!