政府網站 SSL 體檢

唐鳳政委辦公室副研究員 莊秉倫

檢查對象

- 機關首頁
  - www.*.gov.tw / *.gov.tw
- 其他四院
- 所屬 Domain
  - **.edu.tw / **.gov.tw
  - 延伸子網域
    - 例如 dict.revised.moe.edu.tw
  - 可以透過 DNS Log 產生清單
    - 101.101.101.101（TWNIC）
    - GSN DNS Server（NDC）

檢查項目 – certificate chains 完整性

- 部分終端裝置可能沒有完整納入政府根憑證
  - 例如 macOS / iOS / iPad 之Safari
- Client 會直接出現憑證錯誤
- 曾經壞掉的範例(已經修復)
  - https://terms.naer.edu.tw

管理員可透過 SSL Labs 檢查

檢查項目－Portocols

- TLS 應 1.2 以上
  - 相容性清單 https://caniuse.com/?search=TLS
  - 可依照受眾決定是否要保留 TLS 1.0 / TLS 1.1
- 可以開始考慮支援 TLS 1.3
- HSTS Header
  - max-age 可以設定 1 年或與憑證最長有效期相等

檢查項目 － HTTP 重導向 HTTPS

- 使用 server-side 301 重導向
  - Google SEO
  - 推薦搭配 HSTS 一起使用
- 其他方法
  - 透過 meta tag（Mozilla 指出可能會有無障礙網頁議題）
  - 透過 JavaScript（極度不推薦）
    可能有無障礙網頁、SEO 問題

參考：Redirections in HTTP - HTTP | MDN

延伸議題－HTTP 無服務

- HTTP 無服務
- HTTPS 服務無使用 HSTS

使用者需手動輸入「https://」才能抵達網站（Chrome 90+ 已解決此問題）

建議

- 啟用 HSTS
- 可考慮啟用 HTTP 服務，且透過 301 轉向 https

延伸議題－導向到 www

部分網站僅有 www.XXXX.gov.tw

- XXXX.gov.tw 不存在
- XXXX.gov.tw 未正確導向 www.XXXX.gov.tw

建議使用前述 HTTP 導向 HTTPS 所提之方法

延伸議題－重導向到其他 Domain

- HTTP 和 HTTPS 的重導向行為應一致
  - 反例 www.5pc.gov.tw
    - http://www.5pc.gov.tw 導向至 5spc.npa.gov.tw
    - https://www.5pc.gov.tw 導向至TrafficViolationReport.rpb.gov.tw

參考 : Google SEO - Avoid these common pitfalls

延伸議題－Default Server

- 伺服器資訊洩漏
  - 案例 新北市新莊區豐年國小
    www0 露出 IIS 資訊
    - www0.fnes.ntpc.edu.tw
    - www.fnes.ntpc.edu.tw
- 單一服務多組 Domain
  - 案例 新北市立光復高中
    www5 無設定憑證，應直接移除（若有網管需求應改以內部 DNS 處理）
    - www.gfhs.ntpc.edu.tw
    - www5.gfhs.ntpc.edu.tw

延伸議題－Default Server

- IP 資訊之 Domain
  - 有轉跳 140-115-0-213.cc.ncu.edu.tw
  - 未轉跳 140-115-17-70.cc.ncu.edu.tw

可能由網管單位設置，網頁管理員（IP使用者）未掌握該 domain 指向自己所管理之伺服器。（尤其 edu.tw 因網管需求擁有大量此性質之 Domain）

IIS 可停用 Default server、nginx 可以回傳 status code 444

延伸議題－內部系統暴露(IP資訊Domain)

- NAS（大宗）
  - http://tn107-116.cop.nctu.edu.tw
  - http://tn107-116.cop.nctu.edu.tw
- 網路印表機（大宗）
  - http://tn106-37.cop.nctu.edu.tw
  - http://ip-120-125-14-232.mcu.edu.tw
  - http://ip-216-121.cs.nctu.edu.tw
- 網路攝影機
  - http://tn106-187.cop.nctu.edu.tw
- 非公開資料
  - TEJ 資料庫 http://203-71-116-115.cjcu.edu.tw
- Infrastructure
  - ESXi 節點 http://ip-120-125-10-52.mcu.edu.tw

其他議題－鄉鎮公所官網變成監視器畫面？

- 海康威視（使用預設帳號密碼）
  - 清單（部分列出，均指向 114.35.154.194）
    - haitu.gov.tw
    - chengkung-house.gov.tw
    - cs-house.gov.tw
    - jinfong-house.gov.tw

議題討論

- 全面檢查方式
  - 中央統一掃描
  - 所屬機關自行掃描
  - 各層 DNS 管理者自行掃描
  - 或是其他..?
- 如何維持
  - 資安或資管處既有管考流程
    - 異常修復期限
  - 定期掃掃描
    - 頻率
  - 或是其他..?
- 延伸 - DNS 管理