宜蘭區域網路中心管理委員會第 35 次會議會議紀錄

壹、會議時間：中華民國 115 年 6 月 24 日（週三）中午 13:00 ~ 15:00

貳、會議地點：國立宜蘭大學圖書大樓一樓 135 會議室

參、會議主席：吳寂絹館長

肆、出列席人員：如附件

伍、會議報告：莊智傑　　會議記錄:吳文達

陸、報告事項：

一、宜蘭區網中心業務報告

1. 雲端伺服器服務與到校服務

(1).雲端伺服器服務現況：聖母專校 DNS 伺服器已完成匯入，Web Server 上線作業持續進行中；慧燈中學因遇到技術問題，目前由區網人員進行克服中，預計暑假期間到校實施現場作業設定。

(2).到校服務時程：預定於暑假 7－8 月到校服務，各學校如需調整月份，可與區網協調。服務重點項目分為三項：

①成功大學向上集中計畫年度維運報告：請各校事先取出報告書，並以 mail 或 LINE 方式先行提供給區網，到校時一同討論報告書內容。

②連線單位 BCP（資安事件通報與應變）演練：今年將與年度維運報告一併進行，預計到校服務時間較往年稍長。

③校內網路與資安相關議題研討：各學校如有相關議題需討論，可提出。

(3).到校服務時程安排：已預定各校到校日期，請各校確認是否有衝突，如有需調整，請儘早提出，區網將盡量配合協調互換。

2. 網站弱點掃描與個資掃描

(1).EVS 弱點掃描服務方面：

①聖母專校：本次掃描發現高風險漏洞 7 個、中風險漏洞 9 個，數量偏高，需特別注意；校方補充說明:主要原因為套件版本問題，廠商（黑快馬）已在處理中，維護合約有效，預計近日完成修補。

②佛光大學：有高風險及中風險漏洞，請盡速修補。

③羅東高中：高風險漏洞仍待確認處理狀態，請儘快修補。

④慧燈中學：高風險漏洞仍待確認，請盡速處理。

(2).個資掃描服務方面：111－114 年個資掃描中高風險比例已從 41%下降至 13.3%，成效顯著；惟建議各校評估網站檔案是否過多，定期刪除過期資料，並特別注意

SQL Injection 漏洞部分，目前情資通報比例仍偏高，如有發現請盡速檢視並執行修補作業。

3. 宜蘭區網骨幹升級至 400G 說明

(1). 進度現況：教育部設備與線路已於學術網路機房佈線就緒，預計於 115 年 8 月 17 至 19 日進行服務移轉切換工程。

(2). 切換說明：整體切換時程為 3 天，首先會進行區網服務切換，接下來每個學校線路依序進行切換，連線單位實際斷線時間約 5 至 15 分鐘，整體作業時間每個連線單位不會超過 1 小時，如切換後發現異常，會立即回切，降低網路服務失聯時效。

(3). 架構變更：目前為單 Core Switch 架構，升速後將改為雙 Core Switch，提升備援能力；詳細架構圖預計年底向各校匯報。

(4). 請各校確認 8 月 17 至 19 日是否有重大活動或考試需求，如有衝突請提出，以便協調教育部調整切換時程。

4. DDoS 攻擊事件補充說明

(1). 攻擊概況：6 月初發生兩波 DDoS 攻擊，第一波流量峰值達 35–36G，造成部分學校連線不穩；第二波因已掌握攻擊手法，流量清洗中心接獲通知後即時清洗，影響較小。經觀察及資訊收集，以攻擊周期角度分析得知，主要集中於每週二進行攻擊。

(2). 識別特徵：異常流量暴增（海量攻擊）、不對稱上下行流量、固定時段或周期性發動。

(3). 請各校平時多留意 MRTG/cacti 流量監測平台，如發現流量異常，請立即通報區網中心協助。

(4). 本次攻擊分析資料將於會後提供給各連線單位參考。

5. CDN 提供 DNS Resolver 服務

(1). 新服務推出：配合 RPD 政策，由 CDN 提供 DNS Resolver 服務，共兩台，具備不當資訊阻擋功能。

(2). 建議各學校將 DNS 設定指向 CDN 提供之 DNS Resolver，以配合學術網路不當內容存取限制。

(3). 如發現誤擋情形，請即時回報，每個不當網站需提出申請方可解除封鎖。

6. 下半年工作重點

(1).持續日常維運及服務、網路及資安諮詢輔導。

(2).推動連線單位 IPv6 導入，配合到校服務執行。

(3).到校服務含 BCP 演練、障礙排除及訓練輔導（含 BCP 演練手冊操作指引）。

(4).協助辦理網路與資安相關教育訓練課程，各校如有需求可提出。

(5).持續推動 EVS 弱掃及個資掃描平台，協助各校進行漏洞修補。

7. Fortinet 防火牆漏洞說明

(1).近期 Fortinet 防火牆存在重大資安漏洞（Fortibleed 攻擊），可能造成憑證外洩，部分學校已收到廠商自動通報。請各使用 Fortinet 防火牆之學校儘速完成檢測與修補。

8. 國教署資安實地查核說明

(1).今年為第二輪最後一年，目前無學校被排定實地查核；惟線上查核仍須繳交相關資料，請各校配合。

(2).查核項目調整：今年查核項目趨向行政院架構，分為策略面、管理面、技術面及認知訓練四大面向，各校應已收到公文說明。

9. 向上集中核心業務維護計畫說明

(1).核心業務列載原則：維護計畫中之核心/非核心業務，若屬教育部或學術機構（如成大）提供、且學校未自行與廠商簽約者，可不列入核心業務。

(2).需列入之項目：學校自行與廠商簽約或自行開發維運之系統，均需列入維護計畫

10. 數位果子網頁系統資安疑慮

(1).數位果子近年多次發生重大資安事件，國教署已進行專案檢查，惟廠商配合度不佳，工程師人力不足，改善成效有限。

(2).國教署已有委員提議將數位果子排除向上集中，目前尚未確定，但不排除未來朝此方向執行。

(3).如數位果子被排除向上集中，原使用學校之網頁將回歸學校自行維護，學校資安責任等級可能提升（如從 D 級提升為 C 級單位），請各使用學校預先評估因應措施。

柒、臨時動議：無

捌、散會：14:00