財團法人台灣網路資訊中心

網路安全委員會第五次會議紀錄

開會時間：九十一年五月十日（星期五）上午 10:00 至 12:30
開會地點：台灣網路資訊中心會議室（台北市羅斯福路二段 9 號 4 樓之二）
主持人：陳年興主任委員
出席人員：
行政院研考會　何全德副處長(請假)　　國防部通信資訊參謀次長室　秦雄飛副處長
交通部電信總局　許錫蘭簡任技正　　中研院資訊所　黃世昆研究員
中華民國網路消費學會　林世華理事長　財團法人資訊工業策進會　鄭祥勝顧問
行政院主計處電子資料處理中心　劉勝東副主任(請假)
中央警察大學　林宜隆教授　　成功大學電機系　賴溪松教授
交通大學資工系　謝續平教授(請假)　台灣大學電機系　雷欽隆教授
中央大學資管系　陳奕明教授(請假)　中山大學資管系　陳年興教授
中華電信數據通信分公司　林慶和科長　數位聯合電信公司　馮志弘經理
昇陽電腦協銷系統工程　　蘇炯心協理　台灣微軟股份有限公司　何俊明經理
台灣網路資訊中心　陳文生執行長、許乃文組長、楊禎葆先生、陳玉萱小姐
台灣電腦網路危機處理中心　陳嘉玫教授、蕭群祐先生、周守廉先生、魏銷志先生、陳宗裕先生、王柔婷小姐

記錄:陳玉萱

一、主席報告

略。

二、報告事項：

1. 求職信病毒及 SQL Injection 弱點報告

報告人：TWCERT/CC 魏銷志

報告摘要：

(1)求職信病毒肇因於 Microsoft Security Bulletin MS01-020，為 MINE-TYPE 處理不當所造成。此病毒變種極多，不需開啟附件，只需預覽信件即會中毒，並會主動將掃毒程式關閉。

(2)SQL Injection 是透過合法連線的入侵行為，最主要之原因是程式設計人員對輸入驗證的忽略或不足。預防方式除確實做到輸入驗證之外，對資料庫的輸出也應進行驗證，因為這些輸入資料往往成為資料庫查詢時的參數，如能了解資料庫查詢時的意義，將可更有效的過濾不合理的查詢內容。

2. Sun Security Solution 報告

報告人：蘇迥心委員

報告摘要：

(1)目前業界採用較多的 security solution 有 Single Sign-on、Host-based Access Control、VPN、Platform Hardening；由於國內在 Extranet 的應用較少，因此較少有採用 Network-based Access Control。

(2)Sun 有專門探討 Role-based Access Control 的 whitepaper。

建議事項：

(1)建議 Sun 能提供 Role-based Access Control 實作過程中的困難或建議給委員們參考。

(2)建議能了解 Sun 內部網路是否有分級控管的制度，使人員完全沒有機會接觸與本身業務不相關的內部資料。

3. TWNIC 委託 TWCERT/CC 執行與 DNS 安全相關之工作任務執行情形

報告人：TWCERT/CC 蕭群祐

報告摘要：

(1)目前 TWCERT/CC 已建立一個 DNS 服務弱點檢測網站，提供 TWNIC 第三層 DNS 客戶免費的基礎檢測服務。

(2)第三層 DNS 客戶若需進一步的檢測服務，則以加入 TWCERT/CC 會員的方式即可獲得相關服務。

建議事項：

(1)建議 TWCERT/CC 能儘快將上年度 TWNIC 委託執行與 DNS 安全相關之資訊，以及工作成果公佈於 TWCERT 網頁，以供一般網路使用者隨時參閱。

(2)建議 TWCERT/CC 與 TWNIC 密切配合完成 DNS 服務弱點檢測網站，並提供 TWNIC 第三層 DNS 客戶免費的整體檢測服務。

三、討論題綱：

1. 求職信病毒及 SQL Injection 系統弱點的因應對策討論

討論摘要：

(1)有些單位在媒體上公佈 SQL Injection 的方式，可能造成使用者不必要的恐慌及困擾，擔心國內如有太多單位發布網路安全相關之訊息，將造成公信力不足，國內需要有一專門單位來擔任發布網路安全相關訊息之角色。

(2)建議可由 TWNIC 網安委員會擔任國內發布重大網路安全相關訊息之角色。原則上可以網路安全委員會的名義發布，或是與代表消費者之網路消費者協會聯名發布。為掌握時效，委員如有網路安全相關訊息，建議於內容擬定後以 E-mail 通知各委員，經由多數委員同意後即可發布。如有需要亦可在報紙之民意論壇上以委員會或是與教授聯名方式發布相關建議。惟仍需慎重考慮發布的時機，以免引起反效果。

(3)網路安全除了網路入侵與病毒之外，也應注意與實體安全有關之訊息。例如此次水荒限水措施可能會對機房之冷卻系統造成衝擊，進而影響系統及網路運作與資訊安全。

(4)針對 SQL Injection 防治工作及有關弱點檢測工具的建議：

A. 各系統、軟體廠商可提供修正程式給 TWCERT/CC，讓所有人都可以在 TWCERT/CC 網站上安心取得最安全正確的修正程式。

B. 建議 TWCERT/CC 可以提供安全的 CGI 程式撰寫範例，以降低 SQL Injection 的風險程度。

C. 建議 TWCERT/CC 發展各項程式碼檢測工具。

決議事項：

(1)下次開會將邀請 NICI 資通安全會報的綜合業務組主任方鴻春主任及技服中心主任辜國隆主任擔任指導委員。

(2)水荒限水措施所帶來資訊安全的影響，建議以委員會的名義撰寫文章投稿在報紙之民意論壇版面上。

(3)建議各系統、應用軟體廠商可提供各類程式碼檢測工具的自動化修正程式給 TWCERT/CC 以及公佈於網站上。TWCERT/CC 亦隨時提供安全的 CGI 程式範本並發展檢查程式。

(4)往後遇到重大網安事件，或可能發生情況的預警訊息，可以委員會的名義發新聞稿，或是與更貼近消費者的網路消費學會聯名發布新聞稿或召開記者會。

2. 擬成立網路安全相關工作小組(Working Group)討論

討論摘要：

(1)初期可先成立一個技術面，一個政策面的工作小組。

決議事項：

(1)委請中央警察大學林宜隆教授擔任 “Internet Security Policy 工作小組” 之召集人；並委請網路消費者協會林世華理事長擔任“網路與消費者權益工作小組” 之召集人。請兩位召集人開始邀集有興趣的成員加入工作小組。

(2)建議請 TWNIC 協助建立工作小組之 mailing list 及提供相關協助。

3. DNS 伺服器安全檢測與防護體系之建制與運作研究計畫案初審

報告人：TWCERT/CC 陳嘉玫教授

報告摘要：如計畫書內容

建議事項：

(1)建議考慮弱點資料庫是否應為公眾可存取之服務？

(2)建議考慮代管主機上可能有數個代管客戶的 DNS，當某些客戶提出掃描申

請，某些不願意時，可能產生的法律問題。

(3)建議考慮檢測結果可能會造成 ISP 客戶與代管 DNS 之 ISP 之間的法律問題。

(4)建議暫時不受理受代管之客戶直接申請掃描服務，如有需要必須透過代管之 ISP 提出申請，TWCERT/CC 掃描機制可透過擋住 IP 的方式來防止客戶自行申請掃描。

(5)建議掃描機制一定要有明確的權責聲明。

(6)建議考慮檢測結果的隱私與保護的機制為何?

(7)建議計畫書應加註三點：A. 掃描落實的方法；B. DNS 代管衍生的各種問題的解決辦法；C. 掃描服務的權責聲明。

決議事項：

(1)建議 TWCERT/CC 依委員們討論之建議事項修改計畫書內容，並於計畫書中提出下列各點說明後通過：

A. 弱點資料庫為內部使用，掃描結果只提供申請者與弱點相關的修正程式與修正建議。

B. DNS 代管所產生的各項問題的可行解決辦法。

C. TWCERT/CC 對掃描結果的保護措施。

D. 訂定明確的權責聲明。

4. 相關單位出席 FIRST 國際會議討論

報告事項：

(1)TWCERT/CC 說明去年參加 FIRST 年會的情形：去年年會 TWCERT/CC 由陳嘉玫教授與黃世昆教授代表參加，N-CERT 亦派代表參加，許多國家紛紛詢問 TWCERT/CC 與 N-CERT 的關係；今年三月 JPCERT 會議，TWCERT/CC 以 FIRST member 的身份參加。

決議事項：

(1)建議 TWCERT/CC 以 FIRST member 的身分主動邀請 N-CERT、GSN-CERT 一同參與本年度 FIRST 年會。

四、臨時動議：

1. 討論微軟是否有主動偵測產品是否為盜版的作法。

討論事項：

(1)微軟公司代表表示日前微軟公司已發出新聞稿澄清相關說法。

(2)建議微軟考慮以第三中立單位為微軟出具聲明較具公信力。

決議事項：

(1)建議國內能推動教育部與微軟簽署全國性的教育版權，以及推動消費者集體

議價等方式，以協助教育單位及一般使用者等以較合理的價格取得合法版權。

2. 討論如何防止 Spam Mail 氾濫的問題。

討論事項：

(1)考慮限制動態 IP 發 mail 必須經由 ISP 的 mail server，不可自行架設 mail server 發信。

(2)但需考慮動態 IP 不可架設伺服器的限制與動態 DNS 服務的立意可能有衝突。

(3)網路消費學會已經著手在推動相關法規的立法。

決議事項：

(1)建議本議題在下次委員會時列為討論題綱之一。

五、散會