‖從資訊長到客戶長 ‖美國星巴克有請AI虛擬咖啡師 ‖迪士尼釋出開源工具

CIO IT 經理人

BUSINESS TECHNOLOGY LEADERSHIP

風雲人物

台科大資管系教授羅乃維 Page 36

勤業眾信風險管理諮詢公司總經理萬幼筠 Page 40

開放架構 讓企業更自由

開放原始碼在商用軟體方面的發展表現優異，包括區塊鏈、SDN，到容器管理等方面；而在硬體開放運算計畫上，也有讓ODM為客戶構建資料中心的趨勢。 Page44

特別報導 Page 56

IoT蒐集到壞資料怎麼辦？

部署在物聯網四周的裝置，有時會因為髒汙而傳送混亂的資料到雲端上。

Page 59

11項未來程式開發的預測

我們的預測應用程式的水晶球，為程式設計人員們的職涯提供了些許的線索。其指出在未來的數年中，程式開發領域的風潮將轉入迂迴轉動難以掌握的情勢中。

Page 65

Sky坐穩英國有線電視寶座

英國最大付費電視播公司的Sky集團，全力發展OTT服務，日前更建構積極打造私有雲平台，加快創新服務的部署速度，持續坐穩英國付費電視服務的龍頭寶座。

04月號 2017・No.70 定價240元

ISSN 2223-4519

9 772223 451006 04

雲端安全再要求 SSL/TLS傳輸應認證

當愈來愈多的企業紛紛擁抱雲端應用的同時，資訊安全的考量範圍就不只是機房或使用者端的設備而已，資訊在傳遞的過程是否有足夠的安全保證，更是值得關切的議題。台灣聯凱衛生醫管研究協會理事長顏志展指出，許多人往往以為只要IT環境只要有採用SSL/TLS加密技術，就可以高枕無憂，但只要沒有設定正確，仍然會讓企業資安處於高風險狀態，必須要進行定期驗證，才能確保SSL/TLS傳輸的安全品質。

德國Achelos有限公司亞太區營運總監鄧永基指出，不管是雲端應用或是物聯網的資訊安全，都已從原先的未加密型態，升級到透過安全元件建立加密機制，透過不同型態的SSL/TLS加密為基礎，成為物聯網運作的信任基礎。

但這些攸關信任基礎的資訊安全技術，大多數人的認知，都是以為只要有用就會很安全。就像早期的企業資安觀念，往往會以為裝了防火牆就很安全。但關鍵在於，就算保全機制的品質很高級，要是設定有缺失，依然不夠安全。

鄧永基指出，現在的無線傳輸設備，其實都有加密機制，但一樣還是會常常發生重要個資被駭客破解的新聞，並不是無線加密技術不安全，而是因為沒有做好正確的設定，重要的資料一樣不安全。

因為早期加密機制的狀況，並沒有一個具體的檢驗方式，用來測試設定方式會不會不夠安全（如密碼強度太弱）。此外，有些環境的資安設定很麻煩，必須要一台一台手動的去設定，而且設定完成後，只要有任何元件被更換，可能就得重新設定。

這種設計原本是為了確保機器的安全，但這麼多的人為操作作為，就難以避免出現人為的疏忽。台灣聯凱衛生醫管研究協會導入德國eHealth之成功案例，一套由法務、標準、傳輸機制、檢驗稽核專家取得所制定出來的檢驗認證程序，並擁有模擬攻擊行為的資料庫，能夠定期稽核公證。如按照一般的資訊安全政策，必須要加密到某種等級時，就應該要能用某種等級來對照，是不是有符合預期的設定值，設法避免人為錯誤的因素，才能讓想像的安全跟落實的安全保持一致。

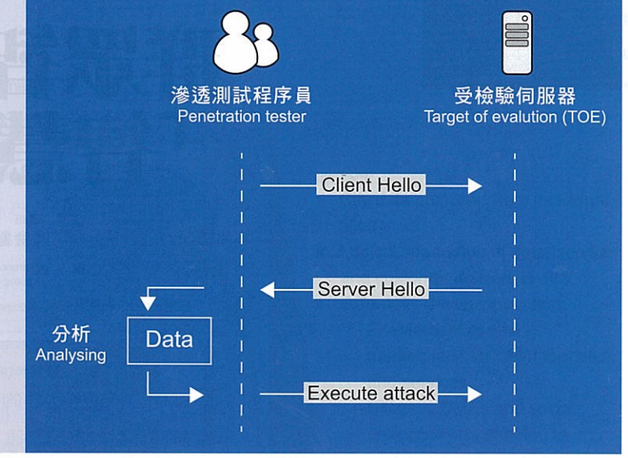
對於資安的依賴，不能只是有安裝SSL/TLS的安全機制而已，而是要能確定每一個環節，都有按照理想值，因為有些人要透明，有些人則是希望安全，設定往往需要符合各方的要求，但如果設定值明明至少要2048，結果輸入的數值卻是1024，雖然一樣有加密，但可能設定上沒有符合應到達的標準。

翔偉資安科技營運長杜世鵬強調，未來上線的物聯網設備會愈來愈多，整體的資訊安全都是建立在某種信任的基礎點，這樣的信任，必須建立在進行定期測試。如果檢測過程沒有真實的執行攻擊測試，使用的協定或產生的紀錄檔就不會產生完整的結論，包括弱點掃描測試、滲透測試等，只要沒有設定好，其實跟沒有設定是一樣的。

台灣聯凱衛生醫管研究協會因此與德國的實驗室(Achelos)合作，導入SSL/TLS傳輸上的認證機制及驗證方案，建立一個可以檢查第四層通訊安全元件的機制，是否有被正確的設定，同時有完全的落實執行。在德國，這套針對第四層的加密的認證機制，包括法制、標準到執行都已經完成，可以套用在伺服器端或是一般的網路設備，確定加密符合要求。

SSL/TLS標準檢驗認證機制

1. 法務、標準規範
2. 模擬溝通封包
3. 加密認證檢驗
4. 執行紀錄及測試認證



鴻毅法律事務所林鴻文律師表示，個資法明文規範保有個資之機關，需建置必要的安全維護設施，來保護個資安全。因此企業如欲免負除法律賠償責任，平時應定期檢測資安措施。而驗證的過程就像是一種掃描機制，會根據作業標準，模擬各種狀況來測試端點與伺服器端的加密情形，並產生紀錄檔，除可用來追蹤測試內容是否符合測試規範外，留存的軌跡紀錄可供查詢修正以及符合法令要求。

林鴻文律師並指出，過去的資安作法有過建立SSL/TLS的管理機制或檢驗方法，最後再成為標準，但如果沒有一套追蹤機制，前面的流程就會變得很被動，所幸現在有了這套追蹤機制，所有的追蹤結果細節都可以顯現出來，就可以讓資安應用單位主動防止資訊外洩。而平常保有大量個資醫療產業，會是第一步推動的方向。

這套驗證機制的公信力基礎，首先是用公規的標準，工具本身也是依照標準協定設計，包括有哪些SSL/TLS機制，有那些攻擊手法會利用那些SSL/TLS的加密漏洞等，而且測試結果至少能夠有個明確的目標，就算有誤判，也能夠很快的回報及更新。其他可以顯示的資訊，還包括能夠檢查安全功能的強度，也就是被攻擊的可能性，以及脆弱點的分析等。

鄧永基指出，驗證機制之所以現在才做，是因為現在的設備效能進步很多，駭客破解的速度變快了，安裝與設定的安全檢測要點繁多，傳統方式要幾位專家耗時數天甚至數週才能完成。德國資訊安全局核可的Achelos檢測工具，只要經過適度培訓的工程師，幾小時最多一天之內可以完成完整的檢測，並提供詳細的報告。

「我們常說IT需要管理，但如果沒有適當的工具，就很難知道哪裡需要管理。」顏志展說：「資料傳輸的安全性，不能只是建立在預設心理，而是要定期認證及複檢。」

事實上，很多人在設定完成後，除非主機出問題，通常不會再去管設定了，真正在做稽核時，也不太可能鉅細靡遺的調出各種資訊，如果能夠過第三方的認證機制，才能協助IT管理人員有無定期檢查安全是否合格。所有的安全，不是有用就可以高枕無憂，安全傳輸機制標準化、檢驗、和認證是未來CIO能證明在安全傳輸機制範圍內有善盡保管之責。