健保局程式碼　相信 Fortify SCA 把關力

撰稿 ：叡揚資訊　行銷總處

守護全台 2,300 萬人的醫療品質，攸關全國人民的健康與福祉，台灣健保局開辦 15 年來，在低保費、低行政經費及高納保率的經營效率，更在國際上贏得好評。例如每人每年所需負擔的醫療費用，美國是我國的 7 倍，日本是我國的 3 倍，以醫療費用佔國內生產毛額計算，我國只有 6.1%，低於絕大多數的國家。

通過政府機關資安滲透測試 建保局很謹慎

值得一提的是，健保局是國內首家取得英國標準協會授權全國認證基金會（TAF）發出的 CNS17800 證照之政府機構。為扎根與落實資訊安全工作，全面推動資訊安全管理系統（ISMS）建置作業；資訊單位分別於 2006 年 3 月及 2008 年 4 月通過國際資安標準 ISO27001 驗證，獲國內外（UKAS &TAF）資安證照各一張，更在去年通過「99 年度政府機關資安滲透測試」，使健保局資安作業全面達到國際標準，完善整體防禦縱深機制。

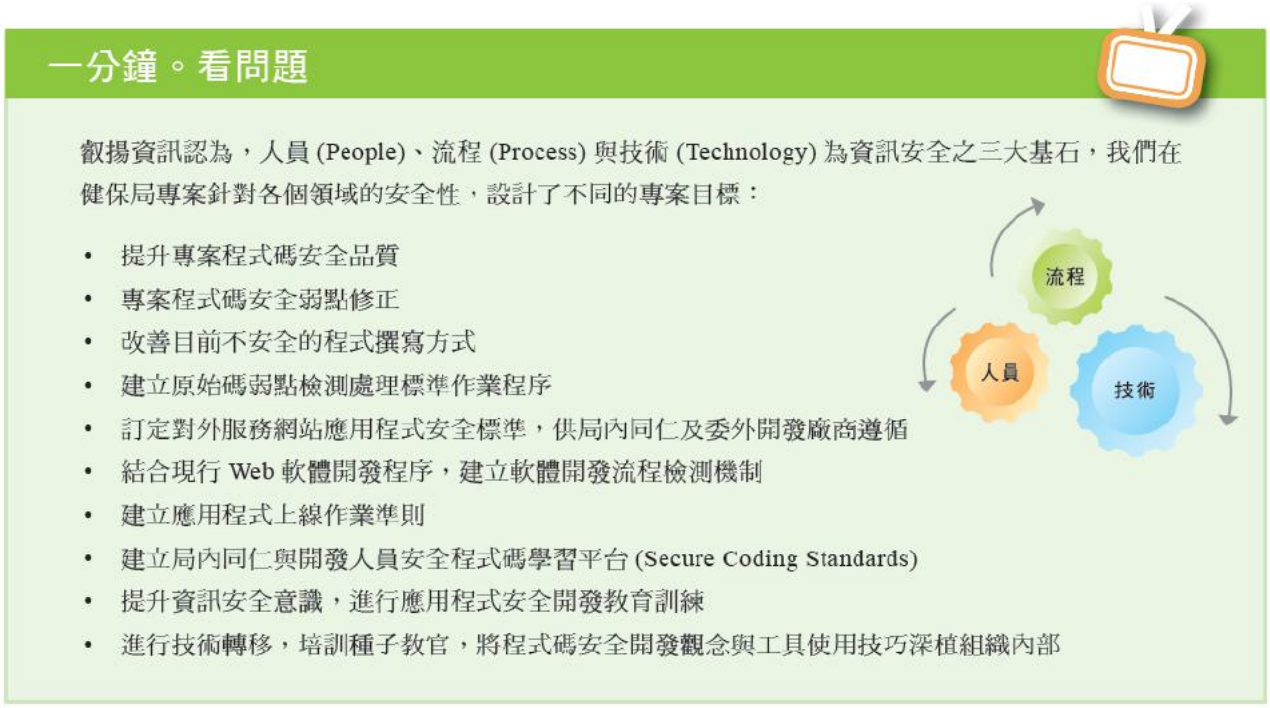
「醫療投保等資料是極為機密之資料！」健保局林志威專員表示說明，早在民國 97 年，健保局就提前預防程式碼漏洞問題，導入市場研究公司 Gartner 評比應用程式安全檢測業界第一：Fortify SCA(Static Code Analyzer)，為程式碼安全作把關。但因應個資法即將上路，《個人資料保護法》除了舊版就有的一般個人資料，更新增敏感性個資的資料類別，敏感性個資包括：醫療、基因、性生活、健康檢查、犯罪前科等資料，讓處理龐大的醫療個資資訊的健保局，更不敢掉以輕心，於今年特地採購第二套 Fortify SCA 強化外包廠商程式碼安全弱點檢測，並訂定對外服務網站應用程式安全標準供局內同仁及委外開發廠商遵循，打造雙層防護、雙管齊下之縝密資安雙認證。

圖說：健保局林志威專員（左）及陳啟舜專員

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

通過政府機關資安滲透測試不馬虎

目前，健保局委外合作廠商約 5~6 家，每個月外包應用程式量約有 100~200 件會送進來，對於編制超過 50 人的資訊組，不但要考量網站使用功能是否完善，還得小心翼翼檢測資安漏洞的疑慮，林志威也強調，隨著個資法即將上路，加強預防更是當務之急。故添購第二套 Fortify SCA，就是專為開發商所建置，並把安全檢測分為三大類:上線檢測、驗證檢測及導入檢測三步驟，同時建立應用程式檢測標準作業程序、上線作業準則及撰寫安全標準，「外包程式上線前，都需要附上測試安全檢測報告，才能核准通過！」林志威解釋，雖然作業多一道程序，但健保局所負責之資訊事關重大，更是需要小心駛得萬年船的心態來經營，才能安全上線！



Fortify SCA＋叡揚顧問　拉高資安外包品質

「把複雜化降至最低、透明度拉到最高，遊戲規則越清晰，健保局及開發商不但雙贏，最重要的是全民醫療個資作把關！」林志威笑笑地說，為了讓工作更有效率、制度更完善，健保局特地協同叡揚以顧問服務方式進行應用程式導入，從建置原始碼檢測平台(含遠端各應用系統程式碼待掃描專區之建構)到檢測程序及作業準則等等及教育訓練推廣，一條龍式的統籌管理，不但保留彈性修正調整，也讓作業安檢程序更具管理制度，「第一，對健保局來說，透過一套完善 SOP 來協助內部檢測作業及管理外包機制；第二，對合作外包商而言，能更清楚開發規則及安全要項。」最重要的是，透過如此嚴謹的 SOP 及教育訓練，讓資安觀念落實在所有同仁及合作廠商，「人人重視資安問題，就成功一大步！」林志威強調解釋。

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

安全類別分等級　標準作業有彈性

當然，針對網站對外對內之功能區別，健保局處理作業也格外細緻，把安全類別通用標準設置為：高、中、低，像是行政資訊科 Internet 全球資訊網系統、保險資訊科網路加退保系統與多憑證網路平台、醫療資訊科健保資訊網服務系統專案等使用 Internet 對外服務之應用程式與網站，因為最容易被有心人士攻擊，故以最高等級的上線標準來檢視；而用 Intranet 對內服務之應用程式並未對外開放，安全需求等級較低，故採用一般等級要求。

Fortify SCA　解決程式碼漏洞專家

另外，擁有 SSCP（Systems Security Certified Practitioner）的專業認證，同時也是(ISC)^2 會員的健保局陳啟舜專員表示，Fortify 就像是程式的健康檢查一樣，透過掃描及顧問諮詢，降低整個軟體專案推動的資安風險。藉由 Fortify SCA 使用於開發階段，可分析應用程式的程式碼是否存有安全漏洞，透過通過程式碼安全分析器找出應用程式可能會執行的所有路徑，SCA 從程式碼中指出安全漏洞。陳啟舜也強調 Fortify SCA 可以在有效的時間內分析大量的程式碼，讓開發人員花費更少的時間與精力來了解和解決問題，讓修復問題變得容易，安全更有保障！

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787