TLP:WHITE

從新加坡醫療資安事件觀察其應處之道

Announcement Advisory Report (ANAR)

2018-08-08

TWCERTCC-ANAR-2018008

TLP:WHITE

Summary

- 新加坡醫療保健集團(SingHealth)資料外洩事件的整體處理流程完善，除了相關政策法規設計得宜之外，也能有效執行資安事件本身的緊急應變，並適時提供民眾正確消息及了解管道，得以降低這次事件影響程度。
- 新加坡整合健康資訊系統公司(Integrated Health Information System, IHiS)對於資安事件有能力偵測並立即採取應變措施，提供相關情資予網路安全局(The Cyber Security Agency of Singapore, CSA)，該局在評估後，依該國網路安全法(Cybersecurity Act)擴大要求其它關鍵資訊基礎設施(Critical Information Infrastructure, CII)同步提升資安防護等級與範圍。

Description

2018 年 7 月 20 日新加坡衛生部(Ministry of Health, MOH)對外表示[1] 新加坡醫療保健集團遭駭，導致 150 萬人的非醫療個人資料(包含姓名、身分證字號、地址、性別、種族及生日)，以及 16 萬名病患的處方等資料遭非法存取及複製。負責管理公共醫療機構 IT 系統的整合健康資訊系統公司於發現新加坡醫療保健集團資料庫異常活動後，立即封鎖異常存取連線，並更換全系統的帳號密碼，新加坡醫療保健集團亦提供專屬網站讓民眾查詢受害情況，使整起資料外洩事件的影響得以降低，其事件時序如圖 1 所示。

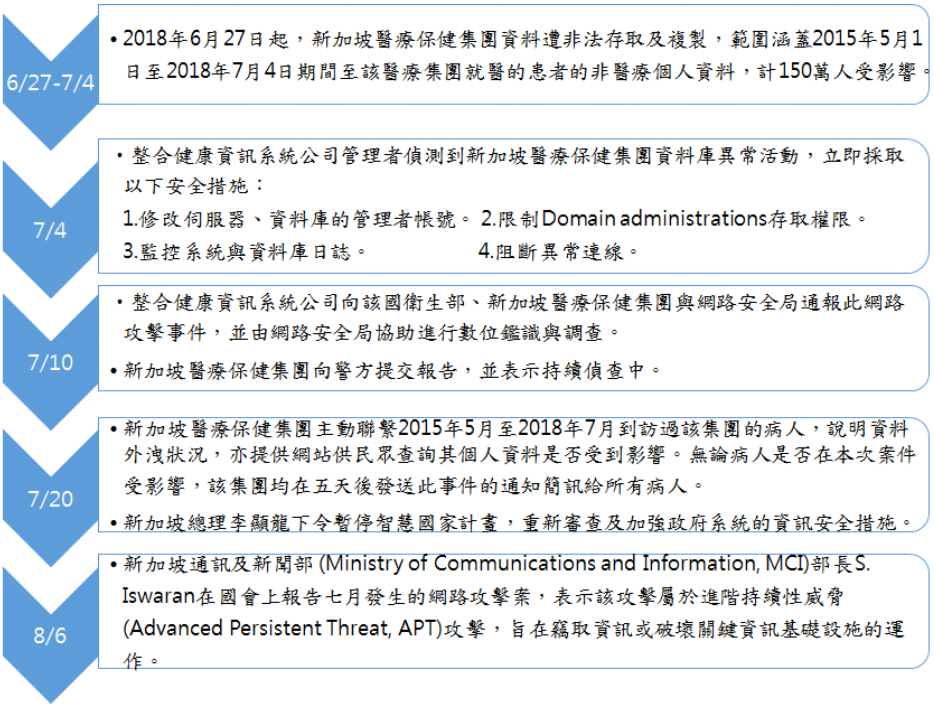

圖 1. 新加坡醫療資安事件時序說明[2][3]

新加坡醫療保健集團與整合健康資訊系統公司雖為民間企業，然而其所維運的病患資料庫是新加坡的關鍵資訊基礎設施之一[2]，一旦受駭足以中斷並影響其正常運作，進而危及國計民生及社會安定。2018 年 7 月 10 日，網路安全局接獲該集團資料庫遭到非法存取的網路攻擊事件之通報後，該局立即部署國家事件應變團隊，支援整合健康資訊系統公司擴大實施必要的安全控制措施，並針對可疑電腦進行數位鑑識與偵查，包含[2]：

1. 阻擋未經授權的連線，以阻止攻擊者存取資料庫。
2. 更換伺服器登入密碼並強制新加坡醫療保健集團內部所有使用者更換密碼。
3. 加強監控所有公共醫療機構的 IT 系統並且實施 Internet Surfing Separation 機制[4]，讓重要系統與網際網路完全隔離。
4. 同步要求所有公共醫療機構的 IT 系統執行以上的安全控制措施。

此資安事件的調查，從 7 月 4 日偵測到異常狀況後，直到 7 月 20 日才由新加坡衛生部對外說明。該部表示[8]，必須經過相當嚴謹的事件確認與處理流程才得以向外界公開宣布此事件的詳情，包含：

1. 必須確認這起事件是一件網路攻擊事件。
2. 必須調查有哪些，誰的資料以及多少資料被竊取。
3. 必須檢查系統，以確保沒有其他數據資料被竊取、破壞、竄改或銷毀。
4. 必須檢查與確認其他所有公共醫療保健系統及政府單位重要系統的安全。

7 月 20 日新加坡衛生部向公眾揭露此資安事件時，已經相當確定系統恢復穩定，同時有準確、足夠的資訊向民眾說明事件如何發生、被竊取的資訊是什麼，以及有哪些人受到影響等相關資訊。

經過數位鑑識調查後，新加坡通訊及資訊部表示[2]：這次事件為國家級駭客組織精心策劃的 APT 攻擊事件，攻擊者利用惡意程式感染前端的電腦系統，以該電腦作為入侵新加坡醫療保健集團網路的突破點，躲避了該集團安全機制的控管及防毒軟體的偵測，並在內部橫向擴散，最終找到存放病患資料的伺服器，在取得系統控制權後，於 2018 年 6 月 27 日至 7 月 4 日期間將資料複製並傳送至海外主機。嗣後，新加坡通訊及資訊部為此召集 4 位專家成立調查委員會(the Committee of Inquiry, COI)來協助調查此事件[2][5]，並要求委員會調查完畢前，不得公開偵查內容。調查委員分別由前首席法官 Richard Magnus 先生、網路安

全解決方案公司 Quann World 的執行主席 Lee Fook Sun 先生、醫療技術公司 Sheares Healthcare Management 的集團首席營運官 TK Udairam 先生和全國工會大會助理秘書長 Cham Hui Fong 女士所組成。由新加坡總檢察署(Attorney-General's Chambers of Singapore, AGC)提供證據給新加坡網路安全局，續由該局帶領團隊進行調查，在調查委員會收到新加坡網路安全局的調查報告後會進行聽證會議，並決定哪些內容可以公開，將於 2018 年 8 月 28 日進行第一次的閉門聽證會[6]，並預計於 2018 年 12 月 31 日由調查委員會報告最終調查結果。

本次事件受駭標的為新加坡的關鍵資訊基礎設施[2]，因此新加坡政府亦要求包含能源、水、銀行與金融、衛生、交通、資通訊及政府機構等其他領域之關鍵資訊基礎設施系統，加強資訊安全防護：

1. 將調查新加坡醫療保健集團系統所得之入侵指標(Indicators of Compromise)與解決方式，提供給各關鍵資訊基礎設施管理者及其監管單位，要求渠等比對與阻檔這些特徵情資。

2. 網路安全局亦要求各領域關鍵資訊基礎設施管理者必須加強其對外網路閘道的安全防護。

為此新加坡政府在 7 月 20 日一度暫停智慧國家計畫，負責推動智慧國家計畫的智慧國家及數位政府工作團(Smart Nation and Digital Government Group, SNDGG)重新審視現有與未來部署的政府系統資訊安全措施，並增加額外的偵測與威脅排除的管控措施後，已在 2018 年 8 月 3 日重啟智慧國家計畫[2]。該事件亦讓新加坡政府體認到 2018 年 2 月所通過之網路安全法中將關鍵資訊基礎設施納管是必要的；該法授權網路安全局針對關鍵資訊基礎設施可採取積極保護措施以迅速應對威脅和突發事件 [7]，使網路安全局得以履行監測和管理國家網路安全工作的職能。

由該事件可看出：新加坡處理事件的整體流程完善且嚴謹，除了相關政策法規設計得宜之外，也能有效執行資安事件緊急應變與通報，並適時提供民眾正確消息及查詢管道，得以避免網路攻擊與資料外洩事件影響持續擴大，值得台灣學習，說明如下：

1. 以網路安全法加強對關鍵資訊基礎設施的保護，避免其受到網路攻擊，授權網路安全局可於發生網路攻擊時立即展開調查，並要求關鍵資訊基礎設施提供者須向網路安全局通報資安事件。

2. 事發單位對於資安事件能及時偵測處理並立即採取應變措施，同時提供相關情資予衛生部及網路安全局；網路安全局亦在評估後擴大要求其它

關鍵資訊基礎設施同步提升其資安防護等級與範圍，以預防類似事件在其他系統發生。

3. 由新加坡衛生部與新加坡通訊及資訊部慎重並準確地發布共同聲明，完整說明此資安事件並提供民眾查詢管道以穩定民心。

Recommendations

針對此類事件，TWCERT/CC 整理 SingCERT[9]所提防護建議，值得台灣納為企業評估重要系統資安防護的參考。

1. 定期檢視網域管理者帳戶及權限

網域管理者擁有其網域的管理最高權限，因此須定期控管帳號權限，若發現異常的管理者帳號應刪除之。

2. 非經授權的遠端存取行為

注意資料庫存取的語法限制，當發生異常的資料庫查詢行為，應有警告機制並注意系統日誌、資訊安全日誌有無異常紀錄。系統及資料庫登入密碼應使用強密碼並定期更換，另應對於重要系統的登入採取多因子認證。

3. 加強管控長時間運行的終端設備

若終端設備長期處在不關機的狀態下，應設有監控或惡意行為偵測機制，另針對未使用的資通訊設備應移除，以減少終端設備遭駭客利用，而成為入侵途徑。

4. 以白名單方式限制使用者可執行的應用程式、服務及來源網路位址

以白名單方式限制用戶可執行的應用程式及服務，可以防止其他未經許可惡意軟體的執行，另針對重要系統亦應以白名單方式限制可連線使用者的來源網路位址。

5. 更新修補程式並保持系統更新

適時更新作業系統及應用程式相關修補程式，可以避免駭客使用已知的漏洞或惡意程式進行攻擊，針對防火牆與防毒軟體等系統防護設備也需定時更新，以確保系統的最佳防護效力。

6. 定期稽核並落實實體隔離防護機制

已實施實體隔離安全防護機制的企業，針對其實體隔離網路架構及隔離機制實際執行情形應定期稽核，並且將所有可連線的設備皆納入風險評估的範圍。

References

[1] Ministry of Health, Singapore. (2018, July 20). "SingHealth's IT System Target of Cyberattack", Retrieved August 16, 2018, from the World Wide Web: https://www.moh.gov.sg/content/moh_web/home/pressRoom/pressRoomItemRelease/2018/singhealth-s-it-system-target-of-cyberattack.html

[2] Ministry of Communications and Information, Singapore. (2018, August 6). "Statement by Mr S Iswaran, Minister-in-Charge of Cybersecurity, on the cyber-attack on SingHealth's IT system, during Parliamentary Sitting, 6 August 2018", Retrieved August 14, 2018, from the World Wide Web: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/8/statement-by-mr-s-iswaran-on--cyber-attack-on-singhealth-it-system-during-parl-sitting-on-6-aug-2018

[3] StraitsTimes. (2018, July 20). "SingHealth cyber attack: How it unfolded", Retrieved August 16, 2018, from the World Wide Web: https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html?utm_campaign=Echobox&utm_medium=Social&utm_source=Facebook&xtor=CS1-10#Echobox=1532093927

[4] Channelnewsasia. (2018, July 23). "SingHealth cyberattack: Internet surfing delinked at all public healthcare clusters", Retrieved August 16, 2018, from the World Wide Web: https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-internet-surfing-delinked-all-public-10555094

[5] StraitsTimes. (2018, July 25). "SingHealth cyber attack: COI members bring variety of expertise, experience to table", Retrieved August 16, 2018, from the World Wide Web: https://www.straitstimes.com/tech/coi-members-bring-variety-of-expertise-experience-to-table

[6] Todayonline. (2018, August 7). "SingHealth cyber attack: First COI hearing on Aug 28, to be closed-door", Retrieved August 16, 2018, from the World Wide Web: https://www.todayonline.com/singapore/singhealth-cyber-attack-first-coi-hearing-aug-28-be-closed-door#cxrecs_s

[7] 上報. (2018, July 23). "江雅綺：前所未見駭人聽聞—星國百萬個資外洩案的啟示", Retrieved August 13, 2018, from the World Wide Web: https://www.upmedia.mg/news_info.php?SerialNo=44963

[8] Mothership. (2018, August 7). "Here's what's the Govt has been doing in response to the SingHealth cyberattack & what we now know", Retrieved August 14, 2018, from the World Wide Web: https://mothership.sg/2018/08/singhealth-cyberattack-ministerial-statement/

[9] SingCERT. (2018, July 20). "Technical Advisory on Measures For Protecting Customers' Personal Data", Retrieved August 9, 2018, from the World Wide Web: https://www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data

聯繫資訊

台灣電腦網路危機處理暨協調中心

- 免付費專線：0800-885-066
- 資安事件通報 03-4115387 或 02-23776418
- 電子郵件：twcert@cert.org.tw
- 官方網站：https://www.twcert.org.tw/
- Facebook: http://www.facebook.com/twcertcc