2020 年 1 月 13 日
討論文件

立法會資訊科技及廣播事務委員會

資訊保安的最新情況

目的

本文件向委員匯報本港資訊保安的最新情況和過去一年政府在資訊保安方面的工作。

背景

2. 資訊科技的普及能為市民帶來方便，提升生活質素，但同時市民、企業和社會受到黑客攻擊的機會亦相應增加。故此，香港要成為安全的智慧城市，不論政府或社會各界以至市民大眾均須對網絡風險有所認識，從而提高警覺，並採取適當措施保護其資訊系統和數據資產，以持續提高整體社會的防範和應對能力。

資訊及網絡安全的形勢

3. 近年來，全球的網絡安全形勢不斷轉變，黑客的攻擊手法亦漸趨多樣化。香港電腦保安事故協調中心（「事故協調中心」）在2019年首11個月共處理8 827宗保安事故，為2018年全年總數的88%，有輕微回落的情況。本港最主要的網絡安全事故類別分別是殭屍網絡（4 570宗）、仿冒詐騙（2 342宗）和惡意軟件（1 205 宗）。有關保安事故的分項統計數字載於附件一。殭屍網絡和仿冒詐騙的宗數有所上升，與全球的網絡安全趨勢大致相同。網絡攻擊多針對系統保安漏洞或用戶警覺不足，並以騙取金錢為主要目的。而殭屍網絡的增加亦為分散式阻斷服務攻擊提供基礎，相關事故數字為35宗，較2018年全年的17宗有顯著上升。據事故協調中心資料，當中大部份個案並非針對香港地區的攻擊，而是收到其他地區報告後處理源自香港的攻擊。惡意軟件的事故宗數在過去一年則顯著下降。

4. 香港警務處(「警務處」)在2019年首三季共錄得4 573 宗科技罪案，是2018年全年總數的58%，有回落的情況，但每宗平均損失金額則有所增加，由2018年約35萬元增加至約49萬元。有關科技罪案的分項數字載於附件二。

社會層面的資訊保安措施

(I) 提升本港企業（包括中小企）應對各種網絡攻擊的能力

5. 政府在2016年推出「科技券計劃」，鼓勵更多本地企業(包括中小企）善用科技，包括提升網絡安全措施以應對網絡威脅。「科技券計劃」已於2019年2月起恆常化和進一步優化，資助上限提高至40萬元，每家企業可獲批項目的數目上限亦由三個增加至四個。「科技券計劃」至今已批核超過150個涉及提升資訊系統及網絡安全的項目，相關的資助金額約1,800萬元。

6. 有別於大企業，中小企未必可分配資源進行防禦網絡攻擊的工作。因此，政府聯同香港互聯網註冊管理有限公司推出中小企網站免費檢驗服務，以協助中小企及早識別潛在的保安漏洞。是項服務除了為持有.hk域名的中小企掃描系統內的惡意軟件和提供資訊保安改善方案外，亦為中小企舉辦多場研討會和工作坊。這項服務自2019年6月推出以來反應熱烈，至今已有約300間本地中小企參與。

7. 此外，因應網絡安全對個別行業的重要性，事故協調中心繼續聯同相關行業的商會舉辦專題講座，進一步向業界推廣網絡安全的意識。過去一年舉辦了超過20次講座，共約2 000名不同界別的從業員參與，涵蓋金融服務、醫療、零售及貿易、物業管理、酒店及旅遊、製造、教育、資訊科技等界別。

(II) 「網絡安全資訊共享協作平台」

8. 政府資訊科技總監辦公室(「資科辦」)在2018年推出「網絡安全資訊共享夥伴試驗計劃」，並牽頭設立跨行業的「網絡安全資訊共享協作平台」(Cybersechub.hk)，促進業界和企業互相分享網絡風險資訊。至今已有約150間公私營機構參與這項計劃，成員機構涵蓋的界別十分廣泛，包括金融與保險、公用事業、運輸、

醫療、電訊、創新與科技、資訊保安、大專院校等。平台讓業界和企業交流網絡安全威脅、緩解方法、良好作業模式等資訊，並設有公開區域，讓公眾也可以獲取專家提供的保安警報和建議。資科辦在2019年11月為這項計劃舉辦了一周年慶祝活動暨專業工作坊，表揚積極貢獻的機構及網絡安全專家，從而鼓勵更多公私營機構參與計劃。

9. 因應參與成員及業界的正面反應，我們決定把這項計劃恆常化，並聯同香港互聯網註冊管理有限公司促進更多公私營機構參與，共享網絡安全資訊。

(III)公眾教育

10. 針對仿冒詐騙的威脅，資科辦、警務處和事故協調中心在2019年舉辦了一系列的宣傳活動，主題為「網絡攻擊花樣多 保護數據靠你我」，以喚起公眾對資訊保安的重視，特別是對數據的保護。資科辦也通過不同渠道，包括網站、社交媒體、文字媒界等，向公眾發放不同種類的網絡安全資訊。

11. 為提升青少年的網絡安全意識，警務處在2019年3月舉行「網樂TEEN才嘉年華」，讓學界了解電腦及流動裝置網絡安全的重要性。資科辦繼續與專業團體合辦學校探訪，於2018/19學年進行了40多次探訪，向逾萬名師生傳遞資訊保安的訊息。

(IV)國際合作

12. 由於香港與全球網絡的聯繫非常緊密，我們必須迅速和有效地應對來自世界各地的網絡攻擊。因此，資科辦與事故協調中心一直積極參與全球及地區性的保安事故協調中心，交流有關網絡安全威脅的資訊及應對措施，以便適時向香港社會各界發出保安預警。資科辦在2019年7月參與由亞太區電腦保安事故協調組織舉辦的年度聯合事故應變演習，以改善各地區應對事故的能力。

資訊保安人力資源發展

13. 隨着網絡安全威脅與日俱增，在2019年本港負責資訊保安及相關職務的人員亦有所增加，總數約為4 200多人，較2018年增加約5%。政府亦會繼續鼓勵大專院校，在不同學科中增設資訊保安課程，以便有穩定的資訊保安人才供應。在專業培訓方面，我們亦聯同資訊保安專業團體向資訊科技人員推廣專業認證，以培訓更多具備資訊保安專業知識和技能的人員。

14. 此外，香港金融管理局與香港銀行學會及香港應用科技研究院合作，推出本地化認證計劃「Certified Cyber Attack Simulation Professional（CCASP）」及網絡安全專業人員的培訓計劃。計劃已獲英國的國際網絡安全認證組織 Council of Registered Ethical Security Testers （CREST）支持，提供具認受性的網絡安全專業培訓。2016年12月至2019年10月期間，共有55名學員通過當中不同級別的考試。

15. 政府在2018年推出「科技人才入境計劃」，為輸入海外和內地科研人才實施快速處理安排。截至2019年12底，創新科技署共批出26個職位範疇屬網絡安全的配額，而入境事務處已根據相關配額批出8宗簽證／進入許可申請予網絡安全人才。此外，政府於2019年公布優化「科技人才入境計劃」，把該計劃的適用範圍擴大至科技園及數碼港園區以外進行研發工作的公司，讓更多本地科技公司就個別科技範疇，包括網絡安全人才的需求，吸納海內外的科技人才。優化計劃的執行詳情將於短期內公布。

政府內部應對網絡安全威脅的措施

(I) 資訊分享及威脅警報

16. 過去一年，資科辦加強收集並分析更多不同來源的網絡安全風險資訊，為各局和部門提供針對性和更適時的預警。資科辦在2019年（截至11月）共發出約90次關於電腦系統或軟件漏洞的保安警報，並要求各局和部門迅速採取適切的防禦措施。

(II) 技術支援

17. 資科辦增設網絡及系統檢測平台，協助各局和部門進行網頁檢測及滲透測試。截至2019年11月底，該檢測平台為約800個政府網站進行測試。我們會為各局和部門的支援人員安排培訓，提升他們對新興威脅的知識及技能。

18. 鑑於仿冒詐騙電子郵件的威脅日益嚴重，政府採用多層保安措施，並加強了政府電郵的保安，方便市民核實政府電郵的真確性，減低遇上偽冒政府電郵詐騙的風險。同時，資科辦利用雲端運算技術建立現代化的中央管理電郵系統，確保參與的局和部門推行更佳的資訊保安管理模式，進一步提高政府內部電郵服務的可靠性和安全性。

(III)員工培訓

19. 政府已制定一套事故應變機制及措施，並定期進行演習，包括每年舉行的大型跨部門網絡安全演習，以提升局和部門應對網絡安全事故的能力。此外，資科辦在2019年5月推行一項為期約10個月的「全政府防範仿冒詐騙演習運動」。演習中所有政府人員均收到模擬仿冒詐騙電子郵件，一旦點擊該些郵件內的連結，相關人員會即時收到反饋，闡釋處理電子郵件的正確方法。我們並透過研討會、專題網站、教學視頻和測驗，介紹如何識別仿冒詐騙的電子郵件和各種常見陷阱，加深員工對仿冒詐騙的認知。

20. 資科辦在2019年舉辦了多個研討會及解決方案展示會，以提升公務員的資訊保安知識。截至11月有超過1 800名政府人員藉此認識最新的網絡安全趨勢及預防措施。資科辦亦鼓勵員工考取國際認可的資訊保安證書，鞏固在資訊保安方面的專業知識。

(IV) 遵行審計

21. 資科辦會定期進行獨立的資訊保安遵行審計，確保各局和部門符合政府的保安規定，並協助他們持續改善保安管理系統，以應對新興保安威脅。資科辦在2019年年中已為政府內部所有局和部門完成一輪的審計工作。新一輪的審計工作已於2019年11月開展，目標是加快於兩年內完成這項定期的審計工作。

展望

22. 因應人工智能、大數據和物聯網等科技的急速發展，資科辦在2019年8月就《政府資訊科技保安政策及指引》開展新一輪檢討工作，涵蓋資訊及網絡安全和智慧城市發展的最新範疇，並參考最新國際標準及業界良好作業模式。我們預期於2020年內完成修訂工作，更新後的指引會公布讓社會各界參考。政府亦會與事故協調中心、香港互聯網註冊管理有限公司及其他持份者繼續合作，進一步提高社會各界對網絡安全及保障個人私隱的認知和能力，為香港構建一個更安全穩妥的網絡環境。

徵詢意見

23. 請委員備閱文件內容。

創新及科技局
政府資訊科技總監辦公室
2020 年 1 月

附件一

香港電腦保安事故協調中心
處理的保安事故分項統計數字

	2018 年		**2019** 年 （截至 **11** 月）		
事故類別	**宗數**	**百分比**	**宗數**	**百分比**	**與 2018 年全年比較（百分比）**
黑客入侵／網頁塗改	59	*<1%*	47	*<1%*	*80%*
仿冒詐騙（釣魚電郵及網站）	2 101	*21%*	2 342	*27%*	*111%*
殭屍網絡	3 783	*37%*	4 570	*52%*	*121%*
分散式阻斷服務攻擊	17	*<1%*	35	*<1%*	*206%*
惡意軟件（包括勒索軟件）	3 181	*32%*	1 205	*14%*	*38%*
其他 [1]	940	*9%*	628	*7%*	*67%*
總計：	**10 081**	***100%***	**8 827**	***100%***	***88%***

[1] 包括身分盜竊、資料外泄等

附件二

香港警務處處理
有關科技罪案宗數及其導致的損失金額的統計數字

	2018 年	**2019** 年 （首三季）	
案件性質	**宗數**	**宗數**	**與 2018 年全年比較（百分比）**
網上騙案	6 354	3 861	61%
（i） 網上商業騙案	*2 717*	*1 686*	
（ii） 電郵騙案	*894*	*604*	
（iii） 網上銀行騙案	*3*	*3*	
（iv） 社交媒體騙案	*2 064*	*1 332*	
（v） 網上雜項騙案	*676*	*236*	
網上勒索	504	255	51%
（i） 裸聊	*281*	*139*	
（ii） 其他網上勒索	*223*	*116*	
盜用電腦 [2]	224	55	25%
其他性質	756	402	53%
總計（宗數）：	**7 838**	**4 573**	**58%**
損失金額（百萬元）：	**2,771**	**2,248**	**81%**

[2] 包括網上戶口盜用、入侵系統活動和分散式阻斷服務攻擊