二零零零年六月十二日
討論文件

立法會
資訊科技及廣播事務委員會

電腦系統被非法入侵和感染病毒的事件以及有關的防範措施

目的

本文向委員簡介電腦病毒、非法入侵及其他干擾電腦保安系統活動所造成的一般電腦保安問題；政府爲保護電腦系統和網絡所採取的防範措施；以及政府對是否有需要在香港成立電腦緊急事故應變小組及其運作模式所作出的考慮。

背景

2. 隨着電腦和互聯網的普及電子貿易日益增長，電腦網絡系統感染病毒、被非法入侵及保安措施受干擾的事故亦越來越多。香港若要在網絡相連的數碼世界中發展成爲電子商貿樞紐，資訊保安是必須重視的課題。

3. 政府十分重視電腦網絡的保安問題，尤其是互聯網的使用。保安問題是設計政府電腦聯網系統所必須考慮的因素，亦是系統發展標準規定程序的一部分。由於互聯網技術的急速發展，我們認爲應付保安事故最重要的措施是加深認識、保持警覺和採取防範措施。

政府為對付電腦病毒而採取的措施

4. 資訊科技署爲政府決策局和政府部門的電腦用戶提供技術支援以應付電腦病毒。該類支援包括印發技術通告和通訊，及定期舉辦研討會和展覽以增加應付電腦病毒的知識。

5. 資訊科技署亦與防毒軟件開發商和本地防毒服務供應商保持密切聯繫，以取得可能的病毒襲擊的最新資料，以便及時向政府的電腦用戶提供意見。資訊科技署亦已建議決策局及政府部門 -

- 安裝防毒軟件以保護所裝設的個人電腦和網絡；
- 定期更新病毒辨識檔案，以便偵察新病毒；及
- 使用病毒掃描設施對新安裝的外來程式或檔案(例如從互聯網下載的程式)進行掃描。

為對付非法入侵政府電腦網絡及對其保安設施作出干擾的活動而採取的措施

6. 爲防範政府的電腦網絡可能被非法入侵及保安措施受到其他形式的干擾，當局採取了四管齊下的方法。

(a) 頒布資訊科技保安政策

7. 我們已頒布一套資訊科技保安政策及相關指引，供決策局及部門採用。

(b) 安裝保安裝置及採取有關程序

8. 我們已安裝防火牆、防毒軟件、偵察干擾活動的系統和其他保安機制，以監察、偵測及阻止懷疑對電腦網絡發動的襲擊。此外，當局亦發展了一套中央互聯網通訊閘系統，讓政府的電腦用戶可以透過中央管理的通訊閘接達互聯網。

(c) 不停監察及管制網絡所收到的通訊

9. 我們利用自動化工具，實時監察及分析在互聯網通訊閘發生的事故。當偵測到涉嫌襲擊事件，便會立即採取行動對抗該等襲擊，並警惕受影響的用戶。

(d) 定期檢討及評估所面對的資訊保安風險

10. 決策局及部門內的系統管理員須定期進行保安評估及審核工作，並不斷地核實及改善電腦網絡系統的保安程度。我們已就該等評估及審核工作的策劃和推行發出詳細指引，供決策局及部門參考。

加深社會各界對資訊保安的認識

11. 資訊科技署密切留意國際和本地組織所提供的電腦保安資料，以掌握電腦保安問題及其解決辦法的最新趨勢。爲加深市民對資訊保安的認識，資訊科技署已經並會繼續與多個工商業組織合辦有關電腦保安的研討會和展覽。

12. 資訊科技署亦製作了一款以「家長認識資訊科技」爲主題的影像光碟，爲家長提供資訊科技教育，以便他們指導子女適當地應用資訊科技。製作該影像光碟的其中一個主要目的，是解釋使用互聯網可能涉及的保安和法律問題。

13. 資訊科技署除會印製有關資訊科技保安的資料單張，派發給市民參考外，亦會在報章上撰寫有關資訊科技保安的文章。我們日後參加展覽時，也會以資訊科技保安作爲其中一個宣傳主題。

14. 至於阻止電腦病毒的散布，資訊科技署已透過有關資訊保安的研討會和展覽，加深市民對這方面的認識，並在提供資料的有關方面同意下，透過傳媒及該署和政府資訊中心的網站，向市民發布防毒資料。該些資料包括描述常見的病毒和惡作劇、防毒指引、新病毒警告，及解答上述各方面的常見問題。資訊科技署的網站亦備有防毒軟件，供市民免費下載。

15. 鑑於電腦感染病毒的情況日益增加，及病毒的破壞力越來越強，資訊科技署亦會加強有關資訊保安的宣傳計劃，包括出版以各種資訊保安問題爲主題的小冊子，及透過傳媒及該署的網站發布更全面的資訊保安資料。

16. 除資訊科技署外，香港生產力促進局及部分大學亦爲社會各界提供資訊保安方面的服務。資訊科技署及香港生產力促進局定期舉辦研討會和展覽，以加深市民對資訊保安的認識。香港生產力促進局亦會於短期內爲已辦理登記的公司提供病毒警告服務。部分本地大學(例如香港科技大學)現正爲一些公司提供資訊保安方面的諮詢服務。

在香港設立電腦緊急事故應變小組的建議

背景

17. 鑑於對電腦系統及互聯網的保安問題的關注，多個國家和經濟體系都設立了電腦緊急事故應變小組，負責發放電腦保安事故報告，及爲受網絡保安事故影響的當地企業和互聯網用戶提供應變方法。電腦緊急事故應變小組一般負責統籌應變及復原行動、找出容易出現保安問題的原因，及採取相應的預防措施。電腦緊急事故應變小組亦會舉辦有關資訊保安的宣傳活動、訓練課程和會議，及與海外的 k 有關機關保持密切聯繫。

18. 電腦緊急事故應變小組在美國創立，原本只負責處理利用互聯網進行研究的機構所遇到的電腦保安問題。Carnegie Mellon 大學替美國國防部管理的電腦緊急事故應變小組統籌中心於一九八八年十二月成立，負責上述工作。自此以後，電腦緊急事故應變小組統籌中心的工作逐漸擴大至包括向公眾發出有關保安事故的警告，及抑制該等事故所造成的破壞。電腦緊急事故應變小組統籌中心於一九九九年共處理超過 8500 宗電腦保安事故。

電腦緊急事故應變小組的組織與職能

19. 我們對若干主要經濟體系[1]所成立電腦緊急事故應變小組的模式進行了初步研究，結果顯示：該等經濟體系所成立的電腦緊急事故應

[1] 已研究的經濟體系包括美國、澳洲、加拿大、英國、新加坡、日本和芬蘭。

變小組主要是非牟利組織，其經費來自業界的贊助、會員費、政府補貼、專上學院的資助，或結合上述各類經費來源。

20. 電腦緊急事故應變小組大多數是負責處理本土保安事故的綜合應變中心，其主要職能包括－

(a) 發出警報及提供意見；

(b) 發布與保安有關的技術資料，及提供/建議採用能預防及偵察保安事故的工具；

(c) 透過舉辦研討會和工作坊來提高各方面對保安問題的認識；及

(d) 與電腦商、資訊服務供應商及其他電腦緊急事故應變小組合作，尋求處理保安事故的方法。

不同國家和地區的電腦緊急事故應變小組所提供的服務各有不同，視乎當地的情況和需求而定。

在香港成立電腦緊急事故應變小組

21. 政府支持仿效多個海外國家的做法，在香港成立由非牟利組織營辦的電腦緊急事故應變小組。

22. 成立本地的電腦緊急事故應變小組，可以－

- 滿足本地的社會及語言需求；

- 集中處理本地社會的電腦保安事故(包括感染病毒及被非法入侵)；

- 及時向電腦用戶發出警報，告知可能存在的資訊保安風險，及提供有關的補救服務；

- 與本地執法機關進行更有效的溝通；及

- 在處理事故時,可作爲與其他組織(包括海外的電腦緊急事故應變小組)聯絡的機關。

23. 成立本地的電腦緊急事故應變小組，可以防止或減少因資訊保安事故而造成的經濟及其他方面損失，從而最終令整體社會受惠。此外，該小組亦可促進資訊科技界、政府、商貿組織與用戶之間的緊密合作。預防資訊保安的風險須要各有關方面的通力合作。政府應協助成立電腦緊急事故應變小組，但該小組的管理和運作則應交由一個非政府及非牟利的組織負責。由於資訊科技(尤其是互聯網)發展迅速，建議成立的電腦緊急事故應變小組必須能夠靈活迅速地配合市場的需求和轉變，及在有需要時招納外界專才。私營機構的參與將有助提供更快捷、富效率和有效的電腦緊急事故應變小組服務。

24. 爲促使市民認識電腦保安問題及研究海外電腦緊急事故應變小組的運作模式，香港生產力促進局已聯同香港科技大學，向創新及科技基金提交有關推行一項教育及培訓計劃的建議。有關的評審委員會

已推薦撥款實行該建議。有關撥款的決定將於短期內公布。香港生產力促進局已計劃派員前赴美國、英國、日本、新加坡及德國，訪問當地的電腦緊急事故應變小組，並會就電腦緊急事故應變小組的運作模式擬備研究報告。此外，香港生產力促進局表示打算於本財政年度內在本港成立一個電腦緊急事故應變小組。

25. 資訊科技署會參與協助在本港成立電腦緊急事故應變小組的工作，並會參與電腦緊急事故應變小組的教育及培訓計劃，以提高市民對電腦保安風險的認識。此外，該署向社會各界發布有關保安事故的消息時，亦會與電腦緊急事故應變小組保持密切聯絡。

資訊科技及廣播局

二零零零年六月

tm381