



HKCERT 資訊保安報

本月內容

- 1.....中小型企業資訊保安指南
- 2.....數據保護
- 10.....保安警告
- 17.....焦點新聞

免費短訊服務

短訊警告服務是新增的免費服務，讓你在何時何地均可接收及時的保安警報，作出相應的防範。

詳情請瀏覽：

https://www.hkcert.org/chinese/subscribe_ssl.html



中小型企業資訊保安指南

香港電腦保安事故協調中心、政府資訊科技總監辦公室及香港警察推出了第三版的「中小型企業資訊保安指南」，內容也增加了對中小企業適用的持續業務運作規劃。



如欲取得此指南

之最新版本，可至本中心網站下載，網址為：

http://www.hkcert.org/chinese/sguide_faq/sguide/sme_guideline.pdf

數據保護

近來數據洩漏的事件層出不窮，引起社會廣泛關注，你有否擔心你個人的或公司的資料外洩呢？你知不知道電腦儲存數據會遇到些甚麼風險？有沒有應對的措施呢？既然大家都如此關心留意這個問題，我們就利用本期的篇幅作個簡介，讓讀者多些瞭解。我們還搜集了一些有用的相關軟件給大家參考，雖然大多是免費軟件，又有很多人使用過，但是，我們還是要不厭其詳，提醒你們，要詳閱軟件的使用條款和適用性，方可使用，還要在安裝任何軟件前做好準備，保護數據和系統。

一些政府和本中心的刊物都是有用的資訊，詳情可參考以下的資料，(見附錄的連結):

- 資訊安全網(InfoSec) 網站
- 中小型企業資訊保安指南
- 政府資訊科技總監辦公室出版的各款小冊子

一. 數據會遇到甚麼風險?

數據遇到的風險主要有三種，分別是數據遺失(Data Loss)、數據損毀(Data Corruption)、數據洩漏(Data Leakage)，造成這三方面的風險的主要威脅來源有：

I. 自然災害

漏水、水浸、火災等自然災害能夠在短時間內對電腦系統及設備造成大規模及永久性的破壞，導致數據遺失。

II. 硬件物理性損壞

各種電腦硬件均有其使用的生命周期，存放不善或使用頻繁均會加速硬件老化；激烈的碰撞也會令硬件損壞，可能造成數據遺失或損毀。

III. 系統失靈

作業系統及軟件發展出更多更強的功能的同時，亦增加系統的複雜性，降低系統穩定性，對數據構成威脅。

IV. 駭客/惡意程式入侵

駭客可透過電子郵件傳播惡意程式或攻擊系統上的保安漏洞，入侵使用者的電腦。駭客會竊取電郵地址及用戶的帳戶和密碼或數據，來勒索用戶、或非法的網上交易或作其他非法用途。

V. 內部人員攻擊

不守紀律的員工或商業間諜，可能在公司內偷取如公司的交易記錄等敏感的資料，出售予商業競爭對手或圖取其他個人利益。

VI. 遺失/被盜

手提型電腦或儲存媒體(如「USB 手指」)都十分輕便，方便隨身攜帶，但亦等如說可以隨處遺失或被竊，數據就有遺失及洩漏的風險。

VII. 人爲錯誤

如果用戶對電腦的認識不足、誤解，或者一時疏忽，均有可能會錯誤地刪除或損毀數據。

二. 如何做好保護數據？

現今的數據是海量的，要耗費龐大的資源去保護所有數據，根本是不切實際的，所以，我們先要知道那些是重要的數據，集中資源保護這些數據，要訂定清晰的管理政策，以有效的程序和工具來執行。

1. 首先要將數據分類，不同重要性的數據需要不同的保護，一般是以數據敏感等級分類 (如機密、內部、公眾等分級)。給部門主管責任，負責為自己部門的數據分級，公司的技術支援部門祇負責執行保護的工作。
2. 分類後，可以按優次制訂保護政策，然後以輔以管理和技術措施執行。
 - 將敏感與非敏感資料分隔，控制敏感資料的存取。
 - 禁止將敏感資料帶離辦公室，或流動儲存裝置上；禁止將敏感的資料放在互聯網上或透過互聯網傳送。如有需要，規定先將檔案加密。
3. 要求員工必須向上級呈報有關數據遺失、損毀和洩漏的事故。
4. 清楚傳遞以上政策的訊息給所有員工。
5. 若公司數據處理涉及第三方，例如維修，應要求對方遵守公司定下的政策去保護數據。若需要的話，可安排上門維修。

三. 針對風險的措施

I. 分隔儲存

分隔儲存是簡單但重要的第一步，第一，我們可以將作業系統與資料分開，方便我們修復系統，例如，如果系統意外受損，或遭駭客和惡意程式成功入侵，需要重灌作業系統時，就不會影響資料存放區。第二，我們可以將敏感資料與普通資料分隔存放，方便系統管理員設置使用權限，減少數據洩漏的風險。

分隔儲存的形式有下列幾項：

i. 儲存在不同的伺服器：

適用於公司內，例如可把人事、財務的數據放在不同的伺服器上，所需的費用較多，但較為安全。

ii. 儲存在不同的硬碟：

適用於桌上型電腦，方便還原系統時，無需觸及數據。維修系統時，亦可將載有數據的硬碟移除，減少數據洩漏的風險。

iii. 儲存在不同的硬碟區：

適用於筆記型電腦，與儲存在不同的硬碟的效果類似，當需要還原系統時，同樣可不觸及數據。不過，維修時不可拆掉唯一的硬碟。

II. 備份

備份是將系統、文件或資料庫系統中的數據加以複製，一旦發生數據事故時，可以容易和及時地恢復系統的有效數據和正常運作。

備份媒體

你要選擇適當的備份媒體，配合你的需要，以下是各種備份媒體的特性和成本的比較。你可以見到，可携性高的備份媒體的保存期較短，要長期保存的數據，還是需要成本較高的磁帶或網絡儲存設備。

	容量	速度(MB/s)	方便	保存期(年)	成本
網絡儲存設備 (NAS)	160GB - 31.2TB	12.5	需 NAS 伺服器及網絡設備	5-10	中/高
磁帶	40GB - 2TB	3.5 - 3600	需擁有可讀取及寫入磁帶的設備	>10	高
外置硬碟	80 GB - 1TB	50	只需連接 USB 的插口	2-7	中
快閃記憶體(USB 手指)	512MB - 8GB	10	只需連接 USB 的插口	1-3	低
DVD	3.95GB - 9.4GB	10	需 DVD 燒錄器	2-5	低
CD	650MB - 800MB	10	需 CD 燒錄器	2-5	低

備份管理

i. 備份的頻率

資料備份並不是一次性的程序，每當資料有所變更便應該進行備份。但若資料經常變更，應定期 (如. 每日或每星期) 進行備份。

ii. 監控過程

備份過程中，可能因為有些檔案被鎖定，導致複製失敗，甚或備份過程終止，導致日後不能完全恢復數據，所以我們應時常檢查備份過程是否成功完成。

iii. 保證備份的可用性

首先，我們要確保備份的數據能夠被復原，所以要定期進行復原測試。

第二，我們要確保在需要復原數據時，能夠快速地檢索出備份的媒體。所以要清楚標示備份媒體(備份日期與備份資料內容)，和建立備份資料的目錄。

iv. 存放環境

大家要留意，不同的儲存媒體對存放環境的要求各有不同：

- DVDR 與 CDR 必須避免陽光的直接照射，避開潮濕及存放化學物品的地方。
- 快閃記憶體與可攜式硬碟必須存放在乾燥與無靜電的環境中。

此外，存放儲存媒體對的實體保安要做好，以免數據被盜。

備份程式

BackupPC (<http://backuppc.sourceforge.net/index.html>) 是一個備份伺服器，讓多名視窗、Linux 及 MacOS 的用戶把數據集中貯存到系統上，視窗用戶可以用視窗共享(Windows file share)方法，Linux 及 MacOS 用戶可以用 rsync 方來備份。

以下還有適合一部機器使用的軟件：

i. 視窗

- NTBackup.exe (系統自帶)
- Areca
<http://areca.sourceforge.net/>

ii. Linux

- rsync (系統自帶)
- Areca

<http://areca.sourceforge.net/>

iii. Mac

– TimeMachine (系統自帶)

– SilverKeeper

<http://www.lacie.com/silverkeeper/license.htm>

– SuperDuper

<http://www.shirt-pocket.com/SuperDuper/SuperDuperDescription.html>

III. 加密

加密是指將易於讀取和理解的資料，透過使用者設定的密碼和經過特定的算法加以轉變，使其變得不可直接讀取和理解，令人看起來是一組無用及難以理解的文本。若要解讀該文本就必需使用相同的密碼解密，恢復至其初始的文本。

檔案洩漏的途徑主要有兩種，第一種是直接從儲存檔案的電腦或記憶設備上被複製出去。其次是在檔案傳送途中(例如電腦郵件傳送)被攔截竊聽。透過加密儲存的檔案及傳送的檔案，可以減低檔案洩漏的風險。

加密的形式和選取

加密的形式有很多種，包括使用作業系統自備的加密功能、外加的加密程式、外置硬件設備等。有些人會利用微軟辦公室軟件提供的加密程式，但這方法很容易被破解，所以不建議用於保護敏感的資料。

i. 加密儲存在本機的檔案:

– 外加的加密程式

外加的加密程式為本機的檔案進行加密時，需要設定密碼，密碼被用作加密算法的密碼匙，在開啓檔案時需輸入同一密碼，將檔案解密。

– 外置硬件加密:

外置硬件加密其實是只把密碼匙放到外置的硬件設備上，只有電腦插入這些外置硬件設備，配合安裝的加密/解密程式才能顯示及開啓已加密的文件，在沒有插入這些設備下這些受保護的文件會處於「隱身」或不能開啓的狀態。

ii. 傳送檔案時加密:

當傳送已加密檔案時，傳送者需要把密碼匙告知收件者，收件者才能將檔案解密，但是在互聯網上交換密碼匙是不安全的，於是衍生了以下兩種的方法。

– 使用不同渠道交換密碼匙:

若使用對稱密碼匙(即加密與解密使用同一密碼)，傳送者需要使用與傳送檔案不同的渠道(如.SMS、電話)把密碼匙告知收件者，從而避免遭人在同一渠道進行攔截而偷得密碼，開啓已加密的資料。

– 公開密碼匙:

利用一對相關但不相同的密碼匙(即私人密碼匙及公開密碼匙對)。傳送者可以利用收件者的公開密碼匙將檔案加密，當收件者接收到檔案就可以利用自己私人密碼匙解密。同樣的公開密碼匙便可以讓不同人士用作傳送機密訊息給接收者，這便解決了需要記下大量共用密碼匙的問題。不過傳送雙方均須協定使用這個機制。

選用安全的加密算法

現時有很多加密程式都提供不同的加密算法給使用者選擇，但一些較舊的加密算法(例如. DES/3DES)已經被破解或不夠堅固，而其他非標準及未被驗證的加密算法也不夠安全。你應選用 AES 或 Blowfish 等加密算法，它們都是由著名的密碼學權威設計的算法，前者更是美國 NIST 選用的新標準算法。

加密程式

i. 視窗

- Truecrypt (免費使用,但不包括其他產品或改變產品)

<http://www.truecrypt.org/>

可加密磁碟區、虛擬磁盤(檔案)及存儲設備

加密算法: AES, Two-Fish

- Blowfish Advanced CS (個人版本)

www.hotpixel.net/software.html

加密算法: AES, Two-Fish, Blowfish

- OTFE

<http://www.freeotfe.org/>

ii. Linux

- Truecrypt

<http://www.truecrypt.org/>

- OTFE

<http://www.freeotfe.org/>

iii. Mac

- FileVault (系統自帶)

- Truecrypt

<http://www.truecrypt.org/>

你需要注意,所有的加密程式或方法都必須設定密碼,若密碼過短或容易被解讀,再複雜的加密算法也變得沒有用,所以應該設定長度適中的密碼。

IV. 數據修復

數據修復是指利用一些工具,還原一些已刪除或損毀的數據。由於在系統移除檔案時,只是清除檔案配置表的內容,實際上所有數據仍然隱藏在硬碟之內。所以若果是不小心的情況下刪除數據,其實可用一些工具還原。

數據修復的程式或工具

- Helix CD

<http://www.e-fense.com/helix/>

Helix 計劃提供一隻免費的開機光碟,內裡載有一些良好的工具去修復及刪除數據。

wipe : 安全刪除文件。

fatback : 分析和恢復已刪除的 FAT 檔案。

dcfldd : dd replacement from the DCFL

以下還有一些工具：

i. 視窗

- PC INSPECTOR File Recovery

http://www.pcinspector.de/Sites/file_recovery/

- Undelete Plus

<http://www.undelete-plus.com>

- DATA Unerase Personal Edition
http://www.octanesoft.com/data_recovery_free_edition.html
- DataRecovery
<http://tokiwa.qee.jp/EN/dr.html>

ii. Linux

- R-Linux (Ext2fs 免費使用)
http://www.data-recovery-software.net/Linux_Recovery.shtml
- DCFLdd
<http://dcfldd.sourceforge.net/>
- Mondorescue
<http://www.mondorescue.org/>

iii. Mac

- R-Studio (這是收費軟件)
<http://www.data-recovery-software.net/>

在一般情況下，軟體故障和硬體故障下數據的成功恢復率一般在 85% 左右。不過在這裡要提醒的是，若發現數據丟失，應立即停止對電腦的一切操作，更不要重複開關機器，否則丟失的數據被覆寫，就會降低數據的成功修復率。

V. 數據永久刪除

前文提及，在系統移除檔案時，只是清除檔案配置表的內容，實際上所有數據仍然隱藏在硬碟之內。就算將硬碟格式化，也不能真正清除硬碟上的資料，因為格式化的指令只是清除每個磁區的使用狀態記錄，確保每個磁區均可使用。要真正清除硬碟資料，就必需重寫每個磁區，將舊有的資料覆蓋。標準的數據刪除和程式，應該合乎如美國國防部的 Data Eraser Standard 522.22-M 標準，其原理是以特定的不同組合的 bit pattern 重寫已被刪除的區隔多次，從而保證數據不能復原。

要確保數據已成功地刪除，可以考慮使用一些措施，如適當的審批程序或記錄方法、抽樣檢查或查證已作數據清除的硬碟。

永久刪除數據的程式

i. 視窗

- Eraser
<http://www.heidi.ie/eraser/>
- SysInternals SDelete
<http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>
- SS Data Eraser
<http://www.ss-tools.com/data-eraser/>
- DBAN
<http://dban.sourceforge.net/>

ii. Linux

- Wipe
<http://wipe.sourceforge.net/>
- DBAN
<http://dban.sourceforge.net/>

iii. Mac

- Mac 系統本身已自帶這個功能
http://www.delamainit.com/articles_how-tos/apple-mac-osx/secure-erase-hard-drive.html

四. 實用軟體表:

	視窗	Linux	Mac
備份	<ul style="list-style-type: none"> - NTBackup.exe (系統自帶) - Areca http://areca.sourceforge.net/ 	<ul style="list-style-type: none"> - rsync (系統自帶) - Areca http://areca.sourceforge.net/ 	<ul style="list-style-type: none"> - TimeMachine (系統自帶) - SilverKeeper http://www.lacie.com/silverkeeper/license.htm - SuperDuper http://www.shirt-pocket.com/SuperDuper/SuperDuperDescription.html
同步備份	<ul style="list-style-type: none"> - Syncback http://www.2brightsparks.com/freeware/ - Unison http://www.cis.upenn.edu/~bcpierce/unison/ - JFileSync http://jfilesync.sourceforge.net/index.shtml 	<ul style="list-style-type: none"> - rsync (系統自帶) - Unison http://www.cis.upenn.edu/~bcpierce/unison/ - JFileSync http://jfilesync.sourceforge.net/index.shtml 	<ul style="list-style-type: none"> - TimeMachine (系統自帶) - SyncTwoFolders (非商業用) http://www.versiontracker.com/dyn/moreinfo/macosx/30727 - JFileSync http://jfilesync.sourceforge.net/index.shtml
加密	<ul style="list-style-type: none"> - Truecrypt (免費使用,但不包括其他產品或改變產品) http://www.truecrypt.org/ - Blowfish Advanced CS (個人版本) www.hotpixel.net/software.html - OTFE http://www.freeotfe.org/ 	<ul style="list-style-type: none"> - Truecrypt http://www.truecrypt.org/ - OTFE http://www.freeotfe.org/ 	<ul style="list-style-type: none"> - FileVault (系統自帶) - Truecrypt http://www.truecrypt.org/
修復	<ul style="list-style-type: none"> - PC INSPECTOR File Recovery http://www.pcinspector.de/Sites/file_recovery/ - Undelete Plus http://www.undelete-plus.com - DATA Unerase Personal Edition http://www.octanesoft.com/data_recovery_free_edition.html - DataRecovery http://tokiwa.qee.jp/EN/dr.html 	<ul style="list-style-type: none"> - R-Linux (Ext2fs 免費使用) http://www.data-recovery-software.net/Linux_Recovery.shtml - DCFLdd (2006 版本) http://dcfldd.sourceforge.net/ - MondoRescue http://www.mondorescue.org/ 	<ul style="list-style-type: none"> - R-Studio (這是收費軟件) http://www.data-recovery-software.net/
數據刪除 (DOD 5220.22-M compliant)	<ul style="list-style-type: none"> - Eraser http://www.heidi.ie/eraser/ - SysInternals SDelete http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx - SSData Eraser (file, folder & disk free space) http://www.ss-tools.com/data-eraser/ - DBAN http://dban.sourceforge.net/ 	<ul style="list-style-type: none"> - Wipe http://wipe.sourceforge.net/ 	<ul style="list-style-type: none"> - Mac 系統本身已自帶這個功能 http://www.delamainit.com/articles_how-tos/apple-mac-osx/secure-erase-hard-drive.html

五. 參考資料:

- 政府資訊科技總監辦公室出版的小冊子:
<http://www.ogcio.gov.hk/>
- 資訊安全網(INFOSEC)的網站:
<http://www.infosec.gov.hk/>
- 中小型企業資訊保安指南:
https://www.hkcert.org/chinese/sguide_faq/sguide/sme_guideline.pdf
- Data Eraser Standard 522.22-M:
http://en.wikipedia.org/wiki/Data_remanence
- 備份媒體的對照表:
<http://www.psyc.vt.edu/kb/kb-0002.html>
- Helix CD
<http://www.e-fense.com/helix/>
- 免費安全(破壞)檔案及磁碟工具
<http://www.thefreecountry.com/security/securedelete.shtml>

HKCERT

電腦保安警報

保安警報					
日期/資料來源	名稱	操作平台/ 軟件供應商	受影響之系統	影響	緩和措施/解決方案
2008/04/07	蘋果 QuickTime 多個漏洞	所有	- 蘋果 QuickTime 7.4.5 之前的版本	- 洩露敏感資訊 - 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/07	思科 Unified Communications 災難復原架構指令執行漏洞	思科	- 思科 Unified Communications Manager (CUCM) 5.x 及 6.x - 思科 Unified Communications Manager Business 版本 - 思科 Unified Precense 1.x 及 6.x - 思科 Emergency Responder 2.x - 思科 Mobility Manager 2.x	- 遠端執行程式碼 - 阻斷服務 - 洩露敏感資料	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/07	Novell Kerberos KDC 多個漏洞	Novell	- Novell Kerberos KDC 1.x	- 遠端執行程式碼 - 阻斷服務 - 洩露敏感資料	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/07	Opera 多個漏洞	Opera	- Opera 5.x - Opera 6.x - Opera 7.x - Opera 8.x - Opera 9.x	- 遠端執行程式碼 - 阻斷服務	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/09	Symantec Mail Security 分析附件漏洞	所有	- Symantec Mail Security for SMTP 5.x - Symantec Mail Security for Domino 7.x - Symantec Mail Security for Microsoft Exchange 5.x	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/09	Lotus Notes 分析 Keyview 多個漏洞	視窗	- IBM Lotus Notes 6.x - IBM Lotus Notes 7.x - IBM Lotus Notes 8.x	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報

日期/資料來源	名稱	操作平台/軟件供應商	受影響之系統	影響	緩和措施/解決方案
2008/04/09	微軟 Visio 多個漏洞	視窗	<ul style="list-style-type: none"> - 微軟 Office XP Service Pack 2 · 微軟 Visio 2002 Service Pack 2 - 微軟 Office 2003 Service Pack 2 · 微軟 Visio 2003 Service Pack 2 - 微軟 Office 2003 Service Pack 3 · 微軟 Visio 2003 Service Pack 3 - 2007 微軟 Office System · 微軟 Visio 2007 - 2007 微軟 Office System Service Pack 1 · 微軟 Visio 2007 Service Pack 1 	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/09	微軟視窗核心漏洞	視窗	<ul style="list-style-type: none"> - 微軟視窗 2000 - 視窗 XP - 視窗伺服器 2003 - 視窗 Vista - 視窗伺服器 2008 	- 權限提高	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/09	微軟視窗 DNS 用戶端 DNS 偽造攻擊漏洞	視窗	<ul style="list-style-type: none"> - 微軟視窗 2000 - 視窗 XP - 視窗伺服器 2003 - 視窗 Vista 	- 偽造	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/09	微軟 Internet Explorer 資料流處理記憶體損毀漏洞	視窗	<ul style="list-style-type: none"> - 微軟 Internet Explorer 5.01 Service Pack 4 · 微軟視窗 2000 Service Pack 4 - 微軟 Internet Explorer 6 Service Pack 1 · 微軟視窗 2000 Service Pack 4 - 微軟 Internet Explorer 6 · 視窗 XP Service Pack 2 · 視窗 XP 專業版 x64 版本 及 視窗 XP 專業版 x64 版本 Service Pack 2 · 微軟視窗伺服器 2003 Service Pack 1 及 微軟視窗伺服器 2003 Service Pack 2 · 微軟視窗伺服器 2003 x64 版本 及 微軟視窗伺服器 2003 x64 版本 Service Pack 2 · 安裝在 Itanium-based 系統中的 微軟視窗伺服器 2003 Service Pack 1 及 微軟視窗伺服器 2003 Service Pack 2 - 視窗 Internet Explorer 7 · 視窗 XP Service Pack 2 · 視窗 XP 專業版 x64 版本 及 視窗 XP 專業版 x64 版本 Service Pack 2 	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報

日期/資料來源	名稱	操作平台/軟件供應商	受影響之系統	影響	緩和措施/解決方案
			<ul style="list-style-type: none"> · 微軟視窗伺服器 2003 Service Pack 1 及 微軟視窗伺服器 2003 Service Pack 2 · 微軟視窗伺服器 2003 x64 版本 及 微軟視窗伺服器 2003 x64 版本 Service Pack 2 · 安裝在 Itanium-based 系統中的 微軟視窗伺服器 2003 Service Pack 1 及 微軟視窗伺服器 2003 Service Pack 2 · 視窗 Vista 及 視窗 Vista Service Pack 1 · 視窗 Vista x64 版本 及 視窗 Vista x64 版本 Service Pack 1 · 適用於 32 位元系統的視窗伺服器 2008 · 適用於 x64 系統的視窗伺服器 2008 · 安裝在 Itanium-based 系統中的 微軟視窗伺服器 2008 		
2008/04/09	微軟視窗 ActiveX 物件記憶體損毀漏洞	視窗	<ul style="list-style-type: none"> - 微軟視窗 2000 Service Pack 4 - 微軟 Internet Explorer 5.01 Service Pack 4 - 微軟視窗 2000 Service Pack 4 - 微軟 Internet Explorer 6 Service Pack 1 - 視窗 XP Service Pack 2 - 視窗 XP 專業版 x64 版本 及 視窗 XP 專業版 x64 版本 Service Pack 2 - 微軟視窗伺服器 2003 Service Pack 1 及 微軟視窗伺服器 2003 Service Pack 2 - 微軟視窗伺服器 2003 x64 版本 及 微軟視窗伺服器 2003 x64 版本 Service Pack 2 - 安裝在 Itanium-based 系統中的 微軟視窗伺服器 2003 Service Pack 1 及 微軟視窗伺服器 2003 Service Pack 2 - 視窗 Vista 及 視窗 Vista Service Pack 1 - 視窗 Vista x64 版本 及 視窗 Vista x64 版本 Service Pack 1 - 適用於 32 位元系統的視窗伺服器 2008 - 適用於 x64 系統的視窗伺服器 2008 - 安裝在 Itanium-based 系統中的 微軟視窗伺服器 2008 	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/09	微軟視窗 VBScript/ JScript 遠端執行程式碼漏洞	視窗	<ul style="list-style-type: none"> - VBScript 5.1 及 JScript 5.1 · 微軟視窗 2000 - VBScript 5.6 及 JScript 5.6 · 微軟視窗 2000 · 視窗 XP · 視窗伺服器 2003 	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報					
日期/資料來源	名稱	操作平台/ 軟件供應商	受影響之系統	影響	緩和措施/解決方案
2008/04/09	微軟視窗 GDI 溢位漏洞	視窗	- 微軟視窗 2000 - 視窗 XP - 視窗伺服器 2003 - 視窗 Vista - 視窗伺服器 2008	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/09	微軟 Project 記憶體驗證漏洞	視窗	- 微軟 Project 2000 - 微軟 Project 2002 - 微軟 Project 2003	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/10	Adobe Flash Player 多個漏洞	所有	- Adobe Flash Player 9.x	- 遠端執行程式碼 - 繞過保安限制 - 跨網站指令碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/15	ClamAV 處理 Upack 執行檔案緩衝區滿溢漏洞	ClamAV	- Clam AntiVirus (ClamAV) 0.92.1 及之前的版本	- 遠端執行程式碼 - 阻斷服務	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/16	ClamAV 處理 PeSpin 及壓縮檔案多個漏洞	ClamAV	- ClamAV 0.93 之前的版本	- 阻斷服務 - 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/17	DivX Player 分析副標題客戶端緩衝區滿溢漏洞	視窗	- DivX Player 6.7 及之前的版本	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/18	CA 產品 DSM "gui_cm_ctrls" ActiveX 漏洞	視窗	- CA BrightStor ARCserve Backup for Laptops 及 Desktops r11.5 - CA Desktop Management Suite r11.2 C2 - CA Desktop Management Suite r11.2 C1 - CA Desktop Management Suite r11.2a - CA Desktop Management Suite r11.2	- 遠端執行程式碼 - 阻斷服務	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報					
日期/資料來源	名稱	操作平台/軟件供應商	受影響之系統	影響	緩和措施/解決方案
			<ul style="list-style-type: none"> - CA Desktop Management Suite r11.1 (GA, a, C1) - CA Unicenter Desktop Management Bundle r11.2 C2 - CA Unicenter Desktop Management Bundle r11.2 C1 - CA Unicenter Desktop Management Bundle r11.2a - CA Unicenter Desktop Management Bundle r11.2 - CA Unicenter Desktop Management Bundle r11.1 (GA, a, C1) - CA Unicenter Asset Management r11.2 C2 - CA Unicenter Asset Management r11.2 C1 - CA Unicenter Asset Management r11.2a - CA Unicenter Asset Management r11.2 - CA Unicenter Asset Management r11.1 (GA, a, C1) - CA Unicenter Software Delivery r11.2 C2 - CA Unicenter Software Delivery r11.2 C1 - CA Unicenter Software Delivery r11.2a - CA Unicenter Software Delivery r11.2 - CA Unicenter Software Delivery r11.1 (GA, a, C1) - CA Unicenter Remote Control r11.2 C2 - CA Unicenter Remote Control r11.2 C1 - CA Unicenter Remote Control r11.2a - CA Unicenter Remote Control r11.2 - CA Unicenter Remote Control r11.1 (GA, a, C1) - CA Desktop and Server Management r11.2 C2 - CA Desktop and Server Management r11.2 C1 - CA Desktop and Server Management r11.2a - CA Desktop and Server Management r11.2 - CA Desktop and Server Management r11.1 (GA, a, C1) OpenOffice.org 2.4 及之前的版本		
2008/04/18	OpenOffice 多個漏洞	所有	<ul style="list-style-type: none"> - OpenOffice.org 2.4 之前的版本 	<ul style="list-style-type: none"> - 遠端執行程式碼 - 阻斷服務 	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報					
日期/資料來源	名稱	操作平台/軟件供應商	受影響之系統	影響	緩和措施/解決方案
2008/04/18	Safari 多個漏洞	Mac	- 蘋果 Safari 3.1.1 之前的版本	- 遠端執行程式碼 - 阻斷服務 - 洩露敏感資料	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/18	Mozilla JavaScript 垃圾收集器漏洞	所有	- Mozilla Firefox 2.0.0.14 之前的版本 - Mozilla SeaMonkey 1.1.10 之前的版本 - Mozilla Thunderbird 2.0.0.14 之前的版本	- 遠端執行程式碼 - 阻斷服務	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/22	ICQ Personal Status Manager 漏洞	視窗	- ICQ version 6 (build 6043) 及之前的版本	- 遠端執行程式碼 - 阻斷服務	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/23	Adobe 產品 BMP 處理緩衝區滿溢漏洞	視窗 /Linux	- Adobe After Effects CS3 - Adobe Photoshop Album Starter Edition 3.x	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/25	思科 Network Admission Control 共享機密漏洞	Cisco	- NAC Appliance software 3.5.x 版本 - NAC Appliance software 3.6.x 版本 - NAC Appliance software 4.0.x 版本 - NAC Appliance software 4.1.x 版本	- 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/28	HP 軟件升級 HPeDiag ActiveX 控制器多個漏洞	視窗	- HP 軟件升級 4.000.009.002 及之前的版本	- 洩露敏感資料 - 遠端執行程式碼	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org
2008/04/29	WordPress Cookie 保護完整性漏洞	所有	- WordPress 2.5.1 之前的版本	- 權限提升	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

保安警報

日期/資料來源	名稱	操作平台/軟件供應商	受影響之系統	影響	緩和措施/解決方案
2008/04/29	StarOffice/StarSuite 多個漏洞	所有	- Sun StarOffice 7 - Sun StarOffice 8 - Sun StarSuite 7 - Sun StarSuite 8	- 遠端執行程式碼 - 阻斷服務	在安裝修補程式時，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。詳情請瀏覽以下網頁： http://www.hkcert.org

* 在安裝修補程式前，請先瀏覽軟件供應商之網頁，以獲取更詳盡的資料。



焦點新聞

0800 免付費電話 變詐騙新手法

2008 年 4 月 1 日

詐騙集團詐騙手法越來越翻新，台中縣一名張姓女子在某知名電視購物台購買東西，購買後接到一通自稱是該購物台人員電話，因來電顯示電話號碼是該購物台免付費電話，加上對方明確說出張女身分證字號及購物內容，張女不疑有他依指示到提款機做轉帳，結果被騙了十幾萬元。提醒民眾如接到顯示 0800 或開頭為 027 的來電，要提高警覺，因為 0800 只能撥進去，不能撥出來，來電顯示 0800 鐵定是詐騙電話。

張姓女子向台中縣消保官翟威甯投訴指出，日前她在某知名電視購物台購買了價值十餘萬元的物品，並以分期付款方式刷卡付費，二天後，貨品還沒收到，卻接到一通自稱是購物台人員的電話，對方聲稱因公司作業疏失，誤將分期付款做成一次扣款，公司已請刷卡銀行做轉正，配合刷卡銀行轉正作業，消費者也必須持卡到提款機再做轉帳動作。

[Yahoo!奇摩]

18 歲\黑客首腦網上盜 1.56 億

2008 年 4 月 2 日

警方透露，18 歲的沃克（Owen Thor Walker）是一個國際黑客組織的首腦，他去年初開始以網名「Akill」犯案，利用自學得來的編寫電腦程式知識，率領一班黑客入侵全球逾 130 萬部電腦，散播病毒及取得用戶資料，共盜取了 2,000 萬美元（1.56 億港元），直至去年底才被警方拘捕，最高可判囚七年。

據悉沃克患有輕度自閉症——亞斯伯格綜合症（Asperger's Syndrome），他出庭當日本無表情。這個病的患者，有人在某些領域上有非凡才能。

[蘋果日報]

美網路詐騙金額創新高 男比女容易被騙

2008 年 4 月 4 日

美國聯邦調查局（FBI）公布的年度報告指出，去年網路詐騙的受騙金額高達 2 億 3909 萬美元（約合新台幣 72.7 億元），創下歷史新高，比前年多出 4000 萬美元。好消息是上當的人數減少，也許美國人學得比較聰明了，但男性顯然比女性容易上當。

美國是十大網路犯罪國家的第一名，占 63.2%。去年 FBI 網路犯罪申訴中心（IC3）接獲的網路詐騙申訴案不到 20 萬 7000 件，少於前一年的 20 萬 7492 件，更少於 2005 年的 23 萬 1000 件。

[Yahoo!奇摩]

商罪科查 FOXY 軟件洩政府機密

2008 年 4 月 7 日

最近外洩的警方內部文件包括內部升級試的試題、警方與逾期居留人士會面紀錄表格，及警務處人員會面紀錄等。這是去年 7 月有傳媒報道多份警員內部文件被人上載於網站，與近期被人以 FOXY 軟件搜尋得到的文件相似。警方表示，商罪科科技罪案組人員正跟進調查事件。

網民是利用 FOXY 軟件搜尋得這些資料，除警方檔案外，民航處的內部文件也可循此途徑搜獲。有讀者向本報指出，只要利用 FOXY 軟件，輸入 confidential 一詞搜尋，即可發現一份名為 confidential memo.dot 的文件，下載後查閱，原來是民航處的文件，上面註明 confidential。

民航處回應稱，該部門的電腦系統完全符合政府資訊科技總監辦公室的保安指引要求，民航處定時進行電腦保安評估及審核，最近一次於去年 11 月完成，結果滿意。就今次有文件外

洩，該部門會進一步調查。有資訊科技界人士指出，網民流行使用 FOXY 搜尋及下載音樂及電影等檔案，雖然方便，但因 FOXY 是共享軟件，一旦安裝等如在電腦加裝了一扇後門，任人進出。

[蘋果日報]

黑客襲擊 aastocks 加強保安追元兇

2008 年 4 月 8 日

本報昨報道香港股民常用的「阿思達克財經網（aastocks.com）」，一度疑遭黑客入侵及加上惡意代碼，致瀏覽網站人士的電腦可能感染木馬病毒，「阿思達克」發言人昨回應時證實確有入侵事件。但他強調前日早上發現病毒後已在短時間內把問題解決，而網站除會加強保安外，亦會調查事件，追究誰是元兇。

阿思達克發言人指出，木馬病毒的問題是由網站的技術人員於前日早上為網站升級時所發現的，但暫未知黑客是如何入侵網站。據資料，今次木馬病毒侵襲的包括台灣國家地理頻道網頁，而木馬病毒疑是源自一個內地網站「414151.com」。電腦保安事故協調中心經理古煒德稱，已知會內地機構，希望對上述病毒網站採取行動。

[明報]

網路購物成犯罪新天地 ATM 轉帳應遵守「三不」

2008 年 4 月 9 日

網路購物詐騙慣用手法，詐騙集團透過管道或截取網路交易訊息，取得民眾網路購物的相關明細後，竄改發話號碼，打給網路購物民眾表示其在網路拍賣店購買物品，於匯款時誤觸分期付款的按鍵，如果不立即取消，每個月到期日都將被扣款，並教導被害民眾如何以 ATM 選擇「英文模式」取消分期付款，被害民眾在

慌張的情形下未加以查證，即依歹徒指示操作提款機，以致被害人存款遭全部提領一空。

詐騙集團詐術花招百出，提醒民眾用 ATM 辦理金融交易，請遵行「三不」須知：1.不要依照別人指示操作提款機。2.不要在電話中向別人告知你的銀行帳號、身份證號碼等個人資料，避免成為「人頭戶」。3.不要聽信歹徒所提供的電話查證，應向 104 或 105 查詢正確的電話號碼，再以電話查證。

[Yahoo!奇摩]

立法 4 月接 2000 投訴 電子信息新招 響一下 誘回電

2008 年 4 月 10 日

電訊管理局 去年 12 月起陸續推出 3 個「拒收信息登記冊」，至今共有 61.1 萬用戶登記，但短短 4 個多月已有 1985 宗投訴，用戶指即使已登記，仍收到商業電子信息。據悉，近日有商戶利用法例灰色地帶，以新招「請君入甕」誘使市民動致電商業機構的宣傳電話。

電管局接到的投訴中，約七成涉及傳真，其次為電郵及預錄電話，分別有 271 及 122 宗，手機短信則有 97 宗。另外，電訊局透露，有 12 宗類似投訴涉及一種新興的商業電子信息傳送方法。

[明報]

網上流傳警隊文件 警稱電腦未被入侵

2008 年 4 月 11 日

本報早前揭發有懷疑警隊內部文件，經點對點 (P2P) 軟件 Foxy 流出。警方指未有發現警務處的電腦系統曾被入侵，但懷疑可能有警務人員未有遵守既定指引處理須保護的資料，商罪科科技罪案組正跟進調查。但記者發現有關文件昨日仍在 Foxy 軟件上流傳，當中更包括警察一直不願對外公開、有關處理槍械與彈藥等較敏感的警察通例章節。

記者昨日再以關鍵字眼在 Foxy 軟件上搜尋，

即再次成功下載上述的警方內部文件，另外更成功下載整套警察通例，當中包括警方一直未肯對外公開、涉及警員處理槍械與彈藥等較敏感部分的警察通例第 16 章。

警方昨日就事件回應稱，根據現時掌握資料，未有發現警務處的電腦系統曾被入侵，但懷疑可能有警務人員未有遵守既定指引處理須保護的資料，又指警方商業罪案調查科 科技罪案組現正繼續跟進調查。但他表示，因仍在調查，當局不便就有關事件進一步評論。

[明報]

賽門鐵克:去年下半年網路釣魚大增 167%

2008 年 4 月 13 日

防毒軟體業者賽門鐵克第 13 期「全球網路安全威脅報告 (ISTR)」指出，在 2007 年下半年，共發現 8 萬 7963 部網路釣魚主機，相較 2007 年上半年，足足成長 167%；而網路釣魚攻擊所瞄準企業中，8% 為金融業。

報告指出，網頁應用程式 (Web) 已成主要攻擊活動管道，越來越多線上使用者僅因造訪常去網站而遭感染。攻擊者利用特定網站弱點作為攻擊跳板；在 2007 年下半年，計有 1 萬 1253 件與特定網站相關跨站攻擊弱點 (Cross-site scripting vulnerabilities) 案例，但僅 473 件 (占 4%) 及時被系統修正漏洞。

[Yahoo!奇摩]

美商週:美政府單位成為網路駭客主要目標

2008 年 4 月 14 日

雖然美國政府已針對網路安全防護加強措施，但多位專家指出，網路的發展非常快速及複雜，防護工作很難面面俱到。美國國防部「高深研究企劃署」在一九六零年代開發出網際網路，國防部已開始思考它是否創造出的是個「怪物」。

報導指出，美國空軍電腦網際指揮部司令羅德曾表示，要打敗美國的對手，也許用不著陸軍、海軍或是空軍，只需用一台個人電腦。

華府方面對於虛擬世界的戰術特別關切還有一項理由 -- 許多新的網路入侵者都是有外國政府在背後支持。報導指出，美國軍方及情報單位人士曾指稱中華人民共和國是美國面對最大的網路威脅。中國在華府的大使館發言人表示，這些指稱都是源自反中國勢力。

[Yahoo!奇摩]

改號軟體氾濫 親友來電可能冒名又冒號

2008 年 4 月 16 日

冒稱親友來電借錢應急、或假稱被人毆打綁架的詐騙案不只在台灣屢見不鮮，大陸也時有所聞，現在騙徒手法更上一層樓，利用所謂「電話號碼修改軟體」，讓受話者手機顯示出「被冒充對象」號碼，讓人更容易上當。

新華網引述大陸「信息時報」報導，這種「冒名又冒號」的詐騙電話越來越多，很多受害人在接到電話時，由於自己手機顯示確實是內建的親友號碼，很輕易就上鉤受騙。

[Yahoo!奇摩]

注意囉! Windows Vista SP1 中文版今起開放 免費網路更新

2008 年 4 月 17 日

從今(17)日起，Windows Vista Service Pack 1 (即 Vista SP1) 繁體中文版開始提供免費網路更新(下載網址：<http://www.microsoft.com/taiwan/windowsvista/sp1>)，而針對 Vista SP1，微軟也將自即日起到 2009 年 3 月 18 日止，提供將近一年的免費支援。

台灣微軟公司營運暨行銷事業群前端平台事業部部門經理葉怡君表示，Vista SP1 並沒有新增功能，而是強化了 Windows Vista 與既有軟體的相容性、效能、穩定度及安全性，而微軟對於 Vista SP1 在品質上的精進深具信心，為了讓消費者能更輕易的體驗這些強化的效能，自今天起提供 36 種 Vista SP1 語言版本(包含繁體中文版)供使用者透過 Windows Update 機制更新，或是獨立下載安裝。

[Yahoo!奇摩]

新世界數據中心故障擾客

2008 年 4 月 18 日

新世界電訊互聯網數據中心因部份客戶用電量過高，導致中心位於葵涌的大廈電源發生故障，網絡服務受影響。有該中心的客戶投訴，事件導致其公司伺服器損毀，嚴重影響公司服務，質疑新世界為何沒有提供穩定電力的設施。

新世界電訊發言人表示，今次事件起因是數據中心部份客戶的用電量過高及超標，導致中心所在大廈的電源出現故障，影響該公司網絡的日常運作。該公司已通知耗電量過高的客戶，酌量調低其寄存於數據中心內的設置耗電水平，否則，不排除於必要時向有關客戶終止供應電力。

[蘋果日報]

百密一疏 網路安全科技量子密碼也有漏洞

2008 年 4 月 19 日

瑞典研究人員今天表示，一般認為能夠完全保護網路資料免受攻擊的新科技量子密碼，依然存在著漏洞。

瑞典南部林雪平 (Linköping) 大學應用數學系助理教授拉森表示：「以電腦術語來解釋，我們發現了程式錯誤的『臭蟲』。」

[Yahoo!奇摩]

報告：熱門關鍵字網頁 安全風險高八倍

2008 年 4 月 21 日

上網搜尋最新話題越來越不安全，根據網頁安全服務業者阿碼科技的最新研究：越是與熱門話題相關的網頁，便越可能帶有惡意程式。

阿碼科技日前(4/16)在台北國際安全博覽會發表了一項針對熱門網頁與惡意程式的關聯性研究，該研究發現，透過搜尋熱門關鍵字所產生的網頁，出現惡意程式的比例，高達 3.31%，若與該公司稍早針對所有台灣網域網站首頁內含惡意程式研究發現 0.42%的比例，兩者差距幾近八倍，若與 Google 今年二月發佈的每一

千個網頁，便有一個帶有惡意程式的研究結果相比，其差距更可達 33 倍之多。

[ZDNet 台灣]

駭客把 Obama 競選網站拐向 Clinton 官網

2008 年 4 月 22 日

上周六晚間造訪 Obama 網站社群部落格區的訪客，都被重新導向 Clinton 的網站。某個網路化名叫「Mox」、自稱來自伊利諾州利物浦的人周日聲稱，是他破解 Obama 的網站。

他低調表示：「我只是利用一些寫得很差勁的 HTML 語法罷了。」基本上，他之所以得逞，是利用所謂「跨網站指令碼」(cross-site scripting)的安全弱點，這種安全漏洞在網站上很常見。一名網路暱稱叫「Zennie62」

YouTube 使用者貼出一則短片，顯示他上 Obama 網站卻被劫持到 Clinton 網站的過程。

[ZDNet 台灣]

全球頂尖黑客：梅鐸聘我竊密碼

2008 年 4 月 25 日

媒大亨梅鐸 (Rupert Murdoch) 的新聞集團旗下公司，被控聘用黑客幫收費電視台入侵競爭對手的衛星系統，竊取加密資料以製造盜版智能卡，導至被入侵公司蒙受巨額損失。涉及案件的一名黑客在加州出庭時承認，他獲梅鐸旗下公司聘用達 10 年之久。

這宗商業間諜案在周三開審。控方 DISH 網絡指出，隸屬新聞集團的 NDS 保安技術公司，入侵 DISH 的衛星網路，竊取加密密碼，然後用偷來的密碼製造盜版智能卡，讓使用者可以越級或免費收看衛星電視，導致 DISH 損失 9 億美元。

[明報]

衛署大懺女醫生 遺下 USB 記憶體被檢走

2008 年 4 月 26 日

衛生署人為疏忽導致大批病人資料外洩，目前

下落不明。一名於屯門兒童體能智力測驗中心工作的大懺女醫生，上周五 (18 日) 遺失存有近 700 名病人及家屬資料的 USB 記憶體，3 日後才由上級報警。衛生署原以為受影響人數只屬「個位數」，至本周三發現病人原來多達 665 人，延至昨日距出事一星期後才公開事件。病人組織批評衛生署及涉事醫生低估事件嚴重性，破壞病人對醫生的信任，提醒受影響病人及家人留意資料有否被不法之途利用，若有損失可循民事途徑向衛生署索償。

該名大懺女醫生於本月 18 日上午在診症室使用該個沒有加上密碼的 USB 記憶體，其間一度離開診症室，但未有將 USB 記憶體收妥及將把門鎖上；她於當日及 21 日仍找不到該 USB 記憶體，同日下午才通知部門主管，翌日報警及通知衛生署。

[蘋果日報]

九龍醫院女護失 USB 事件一年後才公開

2008 年 4 月 27 日

醫院再被揭發遺失存有病人資料的 USB 記憶體。九龍醫院一名女護士於 2006 年 11 月乘車時遺失了一件 USB 記憶體，內存 5 名病人資料，卻因未能確定病人身份而沒有通知當事人，事件交由警方處理，但延至昨日被傳媒查詢下才公開事件，與前日基督教聯合醫院隱瞞遺失 USB 記憶體事件一樣。病人組織批評，事件反映醫管局輕率處理病人資料，漠視病人私隱的重要，以至遺失後不主動呈報，相信同類事件時有發生。

九龍醫院發言人證實，於 2006 年 11 月發生一宗遺失存有醫院檔案的電子儲存媒體 (USB 記憶體) 事件。檔案主要為一般工作文件，涉及約 5 名病人在 5 個月前的紀錄。由於事隔數月，有關職員未能記起檔案涉及那些病人資料，故無法通知病人。院方至今未有接獲病人資料外洩紀錄，而當時已即時通知警方跟進調查。院方已就是次事件採取改善措施，如提醒職員使用加密的電子儲存媒體。

[蘋果日報]

**醫院失「手指」 東區第 4 間
護士長上月遺失 職員指長期插在電腦**

2008 年 4 月 28 日

醫院遺失 USB 記憶體(俗稱手指)事件愈揭愈多，正當醫管局主席胡定旭強調類似事件「不可以再發生」，東區醫院昨日傍晚即爆出有護士長遺失「手指」，成為第四間病人資料失竊的醫院。消息指出，失竊的「手指」由護士長私下購買，用以備存 3 間病房約 60 名精神科病人的病歷私隱。有病房職員說，曾見該「手指」插在電腦上超過一個月，上月 15 日中午失竊後已驚動醫院主管，而肇事護士長仍在病房工作。

本報記者昨午到東區醫院觀察時，發現有部分病房保安寬鬆，外人可輕易進入，且有機會接觸到醫護的電腦。

[明報]

中國駭客攻擊遊戲網站 脅迫配合宣傳

2008 年 4 月 29 日

國內最知名的遊戲討論社群遊戲基地與巴哈姆特，分別遭到 DDoS(分散式阻斷服務)攻擊，來自中國大陸的駭客甚至要求網站配合宣傳，否則將繼續攻擊，行徑令業者咋舌。

擁有眾多使用者的巴哈姆特與遊戲基地網站，自前(27)天起分別傳出因同時湧現大量連線要求導致首頁主機當機事件，其中巴哈姆特甚至收到來自中國大陸、代號 wuwebshell 的駭客來信，要求巴哈姆特刊登其經營的非法線上遊戲伺服器(私服)廣告，否則便會再發動攻擊，巴哈姆特回絕後，竟又在昨(28)日下午受到更強大的攻擊，「沒見過這麼明目張膽的手法，」巴哈姆特站長陳建弘(代號 Sega)說。

[ZDNet 台灣]

公用網路 應做好網路管理

2008 年 4 月 30 日

針對房客可能利用房東提供的網路上網犯罪，網路工程業者吳鎮仲表示，無論是房東或飯

店、汽車旅館業者，提供房客或客人上網設施時應做好內部網路管理，內部 IP 最好使用指定 IP，以利犯罪偵查。

除了飯店、汽車旅館外，目前許多房東出租房子都要強調附設網路設施，才能增加出租率，也有越來越多的餐飲業者提供免費無線上網設施。

[Yahoo!奇摩]

如有任何查詢，請聯絡

香港電腦保安事故協調中心

電話: (852) 8105 6060

傳真: (852) 8105 9760

電郵: hkcert@hkcert.org

網址: <http://www.hkcert.org>