**101**年第1次

北區區網網管會議紀錄

**雲端運算的**

**資料安全探討**

新波科技

劉淂明

Diamond Liu



**雲端運算的資料安全探討**

* 雲端技術的簡介
* 傳統網路的資料安全探討
* Stuxnet – 歷史新發展
* 雲端系統的資料安全探討
* 雲端系統能阻擋多少攻擊?!
* 雲端系統的員工道德操守
* 結論
* Q&A

**雲端技術的簡介**

* 上層分級: 雲端軟體 Software as a Service (SaaS)
* 中層分級: 雲端平台 Platform as a Service (Paas)
* 下層分級: 雲端硬體 Infrastructure as a Service (Iaas)

使用者專注於自身應用需求，而無需擔憂系統相容與品

**雲端技術的簡介**

* 下層分級: 雲端硬體 Infrastructure as a Service (Iaas)
* 中層分級: 雲端平台 Platform as a Service (Paas)
* 上層分級: 雲端軟體 Software as a Service (SaaS)
* 從下層到上層，逐項進行”虛擬化(Virtualization)”。

**傳統網路的資料安全探討**

* 資安三目標
  + 資料:機敏檔案內容，資料庫內容…
  + 資產:軟體，硬體，系統，公司商譽…
  + 隱私:個人網路存取紀錄…
* 資安三威脅
  + 人工式攻擊: 駭客入侵
  + 感染式攻擊: 病毒或蠕蟲，BotNet
  + 內部員工: 檔案竊密，盜賣個資，社交工程
* 防護三步驟
  + 軟硬體安全防護規畫與設定
  + 系統安全監視與內部操作稽核
  + 系統調整與資料備份

**Stuxnet – 歷史新發展**

* 2010-06，歷史上，第一個從個人電腦感染工業(醫療)控制器的跨系統(攻擊型)電腦病毒，相當於生物界的『異種』感染病毒。

**雲端運算的資料安全探討**

**雲端運算的資料安全探討**

* 資安三目標 資料、資產、隱私 沒有改變。
* 資安三威脅 也跟隨到雲端 變得更複雜。
* IaaS，PaaS，SaaS 的重要核心技術之一
* Virtualize (虛擬化) 正遭受駭客努力研究
  + 虛擬機器 Virtual Machine 是否是安全環境?
  + 2006-Blue Pill, Creating undetectable malware on x64 …
  + 2007-SubVirt: Implementing malware with virtual machines
  + 2007-Attacks on Virtual Machine Emulators
  + 2008-Red Pill, Detecting Virtual Machine …
  + 2010? 2011? 2012 ? …

**雲端運算的資料安全探討**

**主機外包廠商會不會有問題?**

* 高科技網路維護公司的工程師的特質
  + 具備網路知識與主機重要訊息(帳號,密碼,檔案)
  + 個人背景因素, 不易查證(就業時無須查證有無前科紀錄)
  + 案例1:奇美電子工程師曾經撰寫木馬程式並且在網路販售,史稱『網路徵信社案件』。
  + 案例2:新竹某國立大學, 研究所學生自製木馬程式販售, 並且偷窺被害人電腦資料, 稱『大鳥木馬案件』。
  + 有無記錄進出機房的整體過程?

(攝影機, 記錄簿, 服務記錄單)

* 有無記錄維護主機的整體過程?

(帳號與身分是否符合? 面部影像? 操作畫面紀錄?)

**雲端運算的資料安全探討**

**Google有多安全?! 信用卡中心有多安全?!**

* 多數雲端技術供應商，其過去產品的資安紀錄，耐人尋味!! Cisco如何? Microsoft如何? Oracle如何?
* 廠商的產品資安紀錄，就如同歷史教訓一樣，會不會重演各種感染病毒蠕蟲與產品漏洞的歷史劇碼呢?
* 一般網管人員最認為安全的Google有多安全呢?資訊安全歷史教訓告訴我們，Google的平台最不易被駭客入侵，但是在2010 三月份，中國大陸的Google公司內部被竊取的是系統加密的公鑰，然後所有重要異議人士的GMAIL電郵信箱內容，逐一被竊!!
* 與其相信某家廠商的產品資安技術，不如假設該資安技術已經被駭客破解，那雲端資料庫內容能否抵擋駭客竊密解譯?

**雲端系統的員工道德操守**

* 雲端系統的管理者，會不會遇到下列問題?
  + 管理者的電腦感染病毒蠕蟲，進而感染其他主機?
  + 管理者的電腦成為駭客跳板，進而連接主機竊密?
  + 管理者的個人私心作祟，進而竊取用戶個人資料?
* 雲端系統的內部稽核系統有多透明?
* 雲端系統的安全監控中心(SOC)能否看到駭客活動?

ps1:多數SOC只是運用IDS/IPS與OS-System的稽核紀錄，進行資料比對，根本沒有人分析網路封包活動!!

ps2:在被入侵的網路環境中，SOC人員經常還在寫報告：表示網路安全一切正常!!

**未來資安的防護要點**

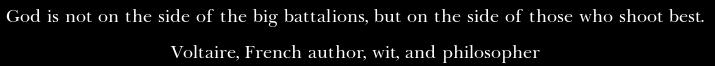
* 安全箴言: 安全防護 不是建立在『駭客的無知』!
* 規則1: 所有資安的防護，從系統自身做起，而非外加式防護！
* 規則2: 任何宣稱100%滴水不露的防護，都是美麗的謊言!
* 規則3: 做好資安，不用花大錢；要有好習慣與對正確的設定!
* 規則4: 當防毒軟體掃描結果，表示無毒的情況，只代表防毒軟體沒有找到病毒檔案，不等於該檔案是乾淨的! (無特徵碼)
* 規則5: 只有相對安全的OS系統，沒有絕對安全的OS系統!
* 慎防 委外系統的漏洞與工程人員的操守問題
* 駭客箴言: 沒有做不到! 只有想不到!

**結論**

* 資安三目標 資料、資產、隱私 沒有改變。資安三威脅 也跟隨到雲端 變得更複雜。
* IaaS，PaaS，SaaS 的重要核心技術之一，Virtualize (虛擬化) 正遭受駭客努力研究。
* 資訊安全制度的規劃，深深影響雲端系統的安全特性，遠勝過任何資安軟硬體產品。
* 破壞資訊安全制度的是人，而不是某項軟硬體產品或是駭客去破壞資訊安全制度。
* 國之將亡，必出妖孽。 駭客之將入侵，必先破壞制度。

**Q&A**

* **Name : Diamond Liu (劉淂明)**
* **Email :** [**dmliu@ms4.hinet.net**](mailto:dmliu@ms4.hinet.net)
* **MSN :** [**dmliu99999@hotmail.com**](mailto:dmliu99999@hotmail.com)
* **Mobile : 0985-604-145**
* **Taipei, Taiwan, R.O.C.**

****

**北區區網網管會議**

**臺灣大學計資中心**

**李美雯**

[**mli@ntu.edu.tw**](mailto:mli@ntu.edu.tw)

**3366-5010**

**大綱**

* **台北區網現況與服務說明**
* **區網中心資安防護**
* **電子郵件社交工程宣導**
* **北區A-SOC學術資安維運中心**

**台北區網現況與服務說明**

* 台北區網大家庭成員
  + 51所大專院校與高中職
    - 歡迎新加入成員台北科技大學
  + 3個單位
  + 台北市教育網中心
  + <http://tprc.tanet.edu.tw/center03.php>
  + 網路流量統計
  + <http://tprc.tanet.edu.tw/mrtg>
  + 台大區網成員使用IP網段
  + <http://tprc.tanet.edu.tw/data/ip_new_ver.php>
  + 後台管理系統
  + <https://tprc.tanet.edu.tw/data_sys/login.php>
  + 各校異動，**請至後台管理系統更新**
  + 網管/資安負責老師
  + 使用網段
  + 新世代骨幹網路
  + 連線速率從100Mbps提昇至1Gbps
  + 提計畫申請書
  + 準備光介面
  + 通過審核後提昇速率之原則
  + FE port連線速率為10Mbps~100Mbps
  + FE port連線速率為100Mbps~1Gbps
  + 臺大區網中心服務窗口
  + 黃怡菁
  + [yichuang@ntu.edu.tw](mailto:yichuang@ntu.edu.tw) 02-33665009
  + 吳廖倫
  + [liaolun@ntu.edu.tw](mailto:liaolun@ntu.edu.tw) 02-33663366 # 51211
  + 李美雯
  + [mli@ntu.edu.tw](mailto:mli@ntu.edu.tw) 02-33665010
* 區網學校與ISP介接
  + 中華電信 Hinet – 1G bps
    - 需擴增1G頻寬
  + 台灣固網 TFN – 1G bps
  + 和信電訊 KGT – 1G bps
* 網路測速上行與下行
  + 中華電信
    - <http://speed.hinet.net/>
  + 中研院
    - 建議測試800M以上的檔案，越大越準確
    - <http://www.ascc.sinica.edu.tw/netsrv/speed/index.php>

**區網中心資安防護**

* 資安技術教育訓練與宣導活動
* 一年多次網站弱點掃描
* 其他服務
  + 「7x24全天候網站掛馬警告系統」服務
  + 網站程式碼弱點掃瞄

**網站資安防護**

* 網站弱點掃描
  + 掃描網站程式弱點，並提供修復建議報告
  + 請自行上網申請掃描<http://mozart.cc.ntu.edu.tw/>
* 網站源碼檢測
  + 找出網站程式碼中的安全問題，並提供修補建議
  + email申請 [yichuang@ntu.edu.tw](mailto:yichuang@ntu.edu.tw)
* 網站安全監控與檢測
  + 計中提供了7x24全天候網站安全監控與檢測服務
  + email申請 [yichuang@ntu.edu.tw](mailto:yichuang@ntu.edu.tw)

**網站個人資料防護**

* 教育機構防洩漏個資掃描平台簡介
  + <https://privacyscan.cloud.ntu.edu.tw/index.php>
  + 個資掃瞄種類
    - 身份證、信用卡、地址、室內電話、手機號碼、E-mail等
  + 可自行設定關鍵個資類別清單
    - 增加個資掃瞄範圍
  + 可掃瞄之檔案格式
    - html、htm、php、asp、aspx、txt、doc、docx、xls、xlsx、pdf、ppt、pptx、jsp
    - 報表功能
    - 提供圖形化分析報表
    - 提供個資洩漏風險分析功能
  + 防洩漏個資掃描平台申請流程
    - 使用者帳號申請
    - 網站檢測申請

**「社交工程」危機意識宣導訓練**

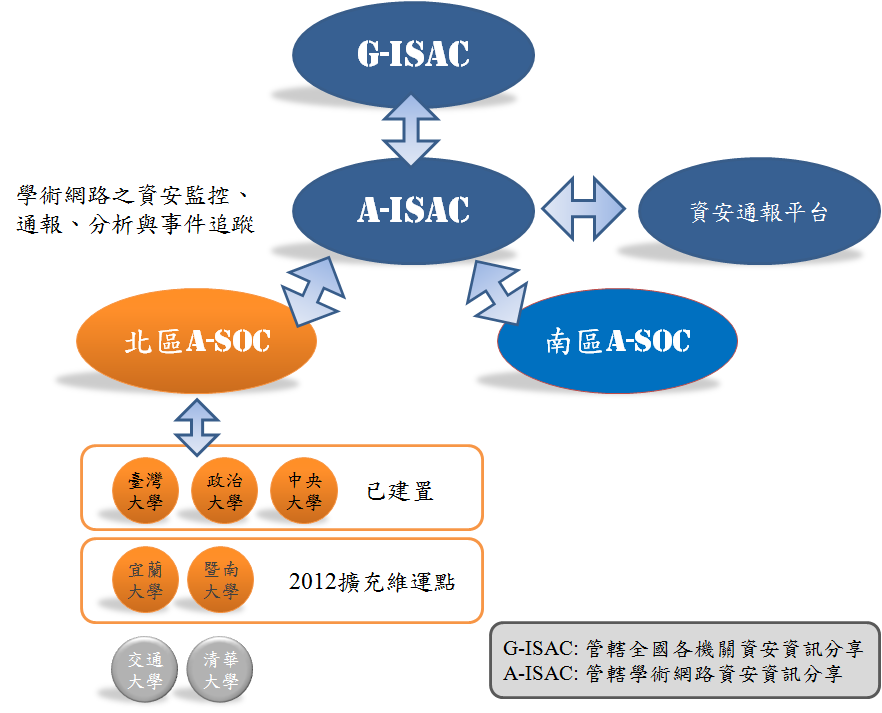
* 各機關人員每年至少須接受
  + 「 1 小時」社交工程防制宣導講習（含 E-Learning 課程）
* 宣導課程應分「兩階段」辦理：
  + 第一階段(於演練作業辦理前)：
    - 對機關所有人員，全面性實施教育訓練
  + 第二階段(於演練作業完成後)：
    - 對開啟惡意郵件或點閱惡意郵件連結或附件之「應重點宣導人員」再次進行宣導，以強化其警覺性

**北區學術資訊安全維運中心**

* 教育部委託於100年7月成立7×24全年無休的北區學術資訊安全維運中心(A-SOC)
* 提供北區學術網路資安事件之偵測、通報與追蹤
* 彙整本校、台北區網中心(台大)、台北區網中心(政大)及桃園區網中心等維運點偵測之資安警訊

**資安維運系統架構**

**安維運點佈建架構**

****

**資安事件分析類型**

|  |  |
| --- | --- |
| **資安事件類型** | **說明** |
| 入侵事件警訊 | 該事件之特徵與證據明確 |
| 資安預警情報 | 證據不充足或可能為入侵事件之前兆 |
| 主動分析  可疑事件 | 每週資安事件量最多之前三名 |
| 資安鑑識 | 重大資安事件；危害學術網路運作，或可能涉及刑事或民事責任者 |

* 連線學校配合事項
  + 確實處理資安事件單
  + 若有任何誤判懷疑與證據，請據實回報以修正觸發規則
  + 網段更改或網管人員/資安人員名單有異動請上網修改並通知北區A-SOC

**問題與討論**