出國報告(出國類別：開會)

參加 THOMVELL 於馬來西亞吉隆坡舉辦之「Cyber Security Asia 2023 Conference」

服務機關：桃園國際機場股份有限公司

姓名職稱：羅曉嵐 (工程師)

派赴國家/地區：馬來西亞/吉隆坡

出國期間：112 年 6 月 18 日至 6 月 21 日

報告日期：112 年 7 月 7 日

目錄

摘要

在現今的科技環境之下，網路攻擊的威脅不斷持續增長，被稱為沒有煙硝的資訊及網路戰爭，從烏俄戰爭證實了資通安全管理的重要性，2022 年 2 月 24 日俄軍攻進烏克蘭邊界的前一日，美國華盛頓的微軟威脅情報中心就偵測到一波針對烏克蘭基礎架構的網路攻擊，發現並阻擋烏克蘭伺服器中一隻新的惡意程式「FoxBlade」木馬病毒，烏克蘭仰賴先進的網路威脅情資與端點保護，成功抵抗多數來自俄羅斯的毀滅式攻擊，儘管戰爭持續延燒，烏克蘭仍持續強化資安管理，外界分析認為，警覺性和創新力是烏國政府資安防護策略的成功關鍵。

THOMVELL 於 2023 年 6 月 18 日至 21 日在馬來西亞吉隆坡舉辦之「Cyber Security Asia 2023 Conference」，提供一個分享交流的平台，由各領域的網路安全專家分享如何應對網路威脅的挑戰及經驗，議題包括網路安全策略、網路風險量化、領導者如何縮短企業在網路安全技能的差距、零信任導入、人類駭客行為學、勒索軟體趨勢等內容，透過專家的知識分享來增進網路韌性，以及保護企業核心所在，有助於精進資通安全的策略面及管理面之規劃。

壹、目的

行程日期	地點	紀要
112/6/18	桃園-馬來西亞 吉隆坡	啟程(JX725) 1010~1455L
112/6/19 至 112/6/20	馬來西亞 吉隆坡 Sheraton Imperial Hotel Kuala Lumpur (喜來登飯店)	本次參與 THOMVELL 舉辦之「Cyber Security Asia 2023」會議，內容包括建置有效的網路方案、未來的人工智慧(AI)學習被用來攻擊網路現有防禦機制、零信任個案學習、網路風險量化評估、AI 仿製員工社群媒體進行網路釣魚，以及公司領導者如何縮短網路威脅及防護的差距等，藉由參與該會議，可瞭解實際發生的網路攻擊事件、未來可能面臨的網路風險，以及如何提升網路安全防護等，進而審視目前公司可能面臨的網路風險、威脅、攻擊的態樣，以及如何建置降低網路風險的防護。
112/6/21	馬來西亞 吉隆坡-桃園	返程(JX726) 1555~2055L

圖一 Cyber Security Asia 2023 會議報到處

圖二 Cyber Security Asia 2023 會議場地

貳、過程

本次會議議題的主講人多數為網路安全領域的實務或學者專家，議題主要圍繞在如何增進或建構網路安全(Cyber Security)的內容，例如：網路安全驗證-Zero Trust、網路攻擊-惡意軟體及從 Human Hacking 的科學角度切入

社交工程等，內容整理如下：

一、網路安全驗證-Zero Trust

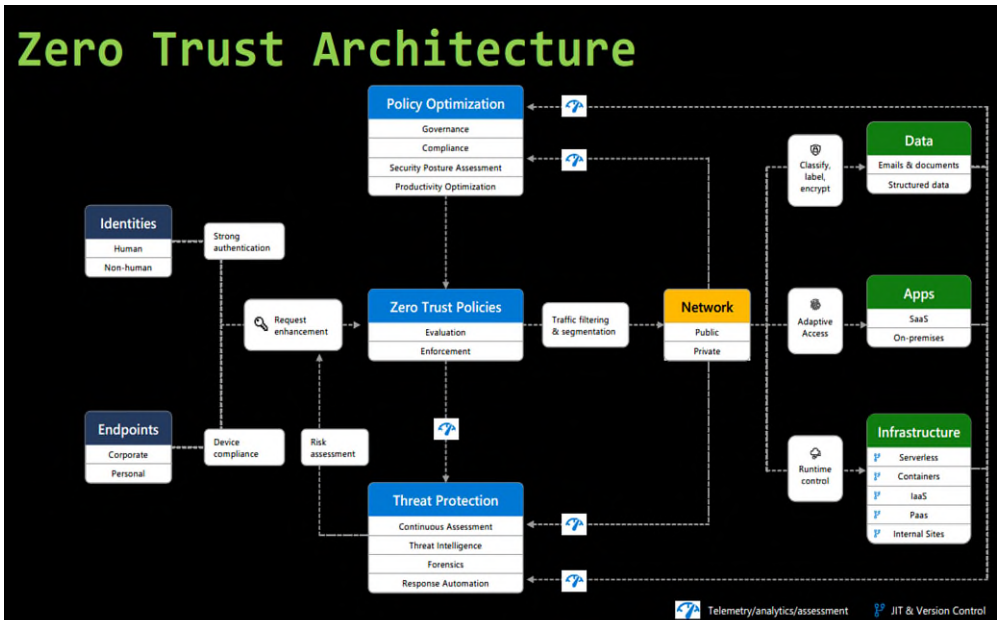
Microsoft 在亞太區的網路安全首席顧問 Abbas Kudrati，說明不要被零信任(Zero Trust)的名稱給誤導，零信任是一個網路安全範例，在零信任(Zero Trust)的框架(圖三)下，是指為了達到可接受的風險或安全水準，信任必須是持續性評估及延伸驗證至各使用者、設備、網路位置，注重在資源的保護與精確，須是持續的評估是否可信任，而不會隱含地授予信任。零信任的原則是假設企業的網路環境是開放的，而不是假設所有東西躲在企業防火牆內就是安全的，因此每個節點都是必須經過驗證始可信任，例如：

(一)攻破假設：假設駭客會成功並進行相應的設計。

(二)明確驗證：對使用者、設備、應用申請、額外的資料取得或遠端資訊服務進行驗證。

(三)使用最小特權訪問：限縮給予授權可能帶來的衝擊。

圖三：零信任架構範例



開始導入零信任前，可先進行的 10 個項目如下：

(一)執行成熟度評估。

(二)為所有人實施條件訪問如：多重要素驗證、無密碼認證。

(三)建置特權管理存取。

(四)對客戶存放在公有雲的所有靜態數據進行加密。

(五)刪除 Windows 使用者的管理員權限。

(六)將終端使用者與數據中心的網絡隔離。

(七)細分關鍵用途。

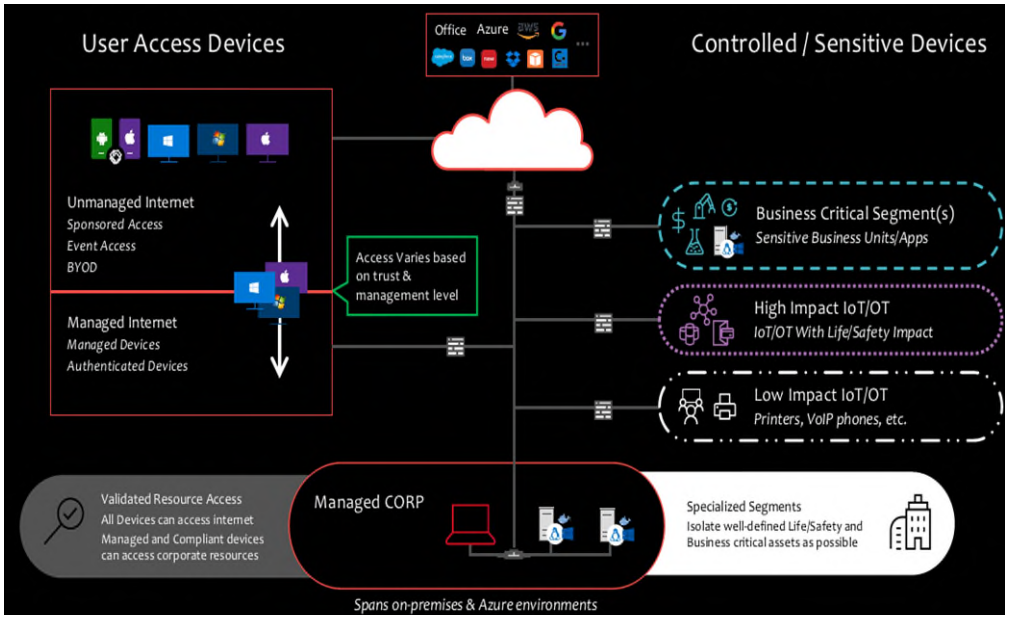
(八)在關鍵服務器上實施鎖定及設定白名單。

(九)對開發人員在開發過程中新增的應用程式進行掃描。

(十)開發人員在部署 Kubernates 集群時，應設置只有管理者可以修改集群的准入控制器而非默認開啟。

從 Microsoft 的個案顯示(圖四)，導入零信任架構後，企業管理跨越本地與雲端的環境，好處是降低用戶和端點受損的風險、提高安全可見性如遠程設備無盲點、跨企業應用程序和服務的單點登錄、可以不分區域進行工作且在安全的防護下，並且改進了”訪問被拒絕”的體驗如對應用程序或數據的訪問權限有限。

圖四：Microsoft – Zero Trust Implementing



二、網路攻擊-惡意軟體

科摩多集團(Xcitium)的 Dr. Erdal Ozkaya 說明惡意軟體(如勒索軟體)，簡單來說就是合法的代碼做非法的事情，代碼是合法的，因為 CPU 可以理解並執行我們稱之為惡意軟件/勒索軟件的可執行文件中的代碼/指令，只是被用來進行非法操作，但如果避免執行檔，則電腦將無法運行。

勒索軟體的盛行主要幾個原因如下：

(一)攻擊者只需要用讀取和寫入權限即可感染被攻擊者。

(二)即使在最小權限使用原則下，攻擊者仍可將資料加密。

(三)在較高權限下，整個組織都可能成為被攻擊的目標。

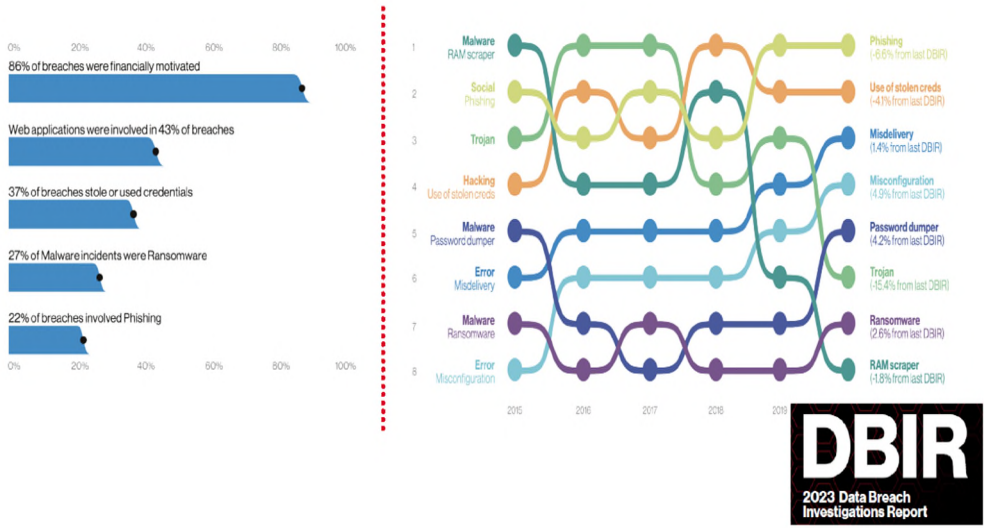
(四)攻擊者容易取得贖金。

(五)只需要 3 分鐘就可以讓被攻擊者無存取被強迫加密的資料。

勒索軟體從 1989 年至 2020 年的歷史，主要的進程是有了加密技術、比特幣和匿名 Tor 網絡，再來就是攻擊者(威脅者)以輕鬆便宜的代價與勒索軟體作者合作且必然取得的投資報酬率，後期則因數據洩漏議題(圖五)而使威脅者能取得更高的贖金如：勒索軟體-GandCrab 作者在一年半內賺進超過 20 億美金，根據美國最大的無線通訊服務供應商(Verizon)

2023 年最新的數據洩漏調查報告也顯示財務是造成違規行為最大的誘因占 86%。

圖五：Verizon 2023 年數據洩漏調查報告



強化網路安全仍然是降低勒索軟體危害的方法，參考美國國家標準暨技術研究院(NIST)的網路安全框架為識別(Identify)、保護(Protect)、偵測(Detect)、回應(Respond)與復原(Recover)，讓企業在管理安全風險時，能夠對應到事前、事中與事後的環節，提供網路安全生命週期的管理策略。

三、Human Hacking

講師 Chris Hadnagy 在一間專門做社交工程演練公司擔任執行長，說明社交工程是影響一個人做出可能符合或不符合其最佳利益的決定的任何行為，並執行 Phising(網路釣魚)達 19,000,000 次，成功率達 75%。在執行社交工程時，非僅統計哪些單位或受測者點擊了連結，亦統計 4 個面向的通報統計(表一)來確認企業的受測員工其資安意識是否達到效果，在這 4 個面向中，就講師的觀點而言，最好的員工是未點擊連結且有主動進行通報。

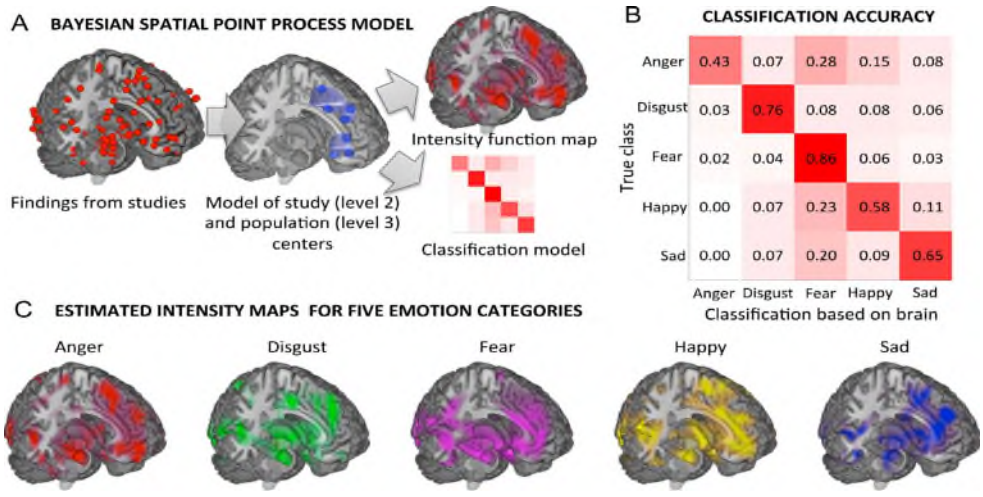
表一：受測者通報統計

Click -> Not Report	Not Click -> Not Report
Click -> Report	Not Click -> Report

該講師主要是透過科學的方法探索我們如何做出這些決定，包含大腦的化學反應或心理狀態(圖六)，然後學習如何利用它們，促使受測的企業員工點擊釣魚信件或簡訊連結，也就是以人類為什麼會受騙點擊連結的角度來進行演說，一般探討到社交工程，通常是透過教育訓練或是社交工程演練來達到資安意識加強，此議題有助於提供不同思考角度及規劃案

例活用在教育訓練或是社交工程演練。

圖六：大腦情緒反應圖



講師從 3 個學術面向進行了解：

(一)Ekman：美國心理學家保羅·艾克曼，主要是研究情緒和面部表情的先驅，情緒刺激由肌肉反應出表情，而表情可以創造情感。

(二)Oxytocin：是一種哺乳類動物激素，是肽類激素也是神經肽，一般由下視丘產生，由腦垂腺後葉釋放。該激素與信任有關，當你感到被信任時更強大而不是當你信任時。

(三)Amygdala Hijack：杏仁核劫持 是一個迅速且壓倒性的情緒反應，往往情緒反應都是過大及過敏，導致更嚴重的情緒威脅。也就是刺激反應發生在大腦啟動之前。

簡單來說，多數受測者在透過大腦正常運作反應前，已先被情緒刺激而提前做出反應，也就是化學反應的釋放會讓自己做出在正常情況下不會做出的決定，從講師測試企業員工的結果顯示，最能誘導受測者信任的過程是刺激擔憂，此時可能已經有部分的人已受騙，若再接著通知第一次未受騙的受測者，以電話通知並正面的讚許未點擊連結後，再度以更深入相關的內容去要求受測員工點擊連結，75%的 Phising 會成功。

最後，面對社交工程的網路風險，講師提供如何提高安全的 4 個提示：

(一)使用科學的角度。

(二)教育資安意識弱項，獎勵正面的行為。

(三)用資訊技術作為防護，但不是用來當救世主。

(四)鼓勵員工看到什麼就說什麼。

參、心得及建議

從本次會議分享的網路安全議題中，發現網路被駭的破口可歸納 3 個原因，分別是現行的網路架構不健全(例如：防火牆規則不明確)、資訊產品本

身的漏洞(例如：程式漏洞)及資安意識不足，建議可從這 3 個原因作為方向來檢視公司現有的作為，再輔以會議中分享的內容來縮短健全網路安全的差距。以公司現行的環境及條件下，雖然不適合全部套用本文分享的內容，然仍有許多值得參考或學習的方向，分享如下：

一、從上級機關的幾場資安研討會的議題中，得知未來資安政策將朝導入零信任(Zero Trust)網路安全框架的方向進行，參考 Microsoft 的導入案例，本公司可先初步著手進行的項目建議如下：

(一)明確定義防火牆規則，防火牆若未依明確規則設定或開放不必要的例外規則，等於開放給駭客未經管制的出入口。

(二)逐步建置多因子驗證或無密碼認證，密碼強化的建議從 4 位元演化到 12 位元，然而駭客透過工具暴力破解並非難事。

(三)引進特權帳號管理 Privileged Access Management (PAM)工具，公司目前在 PC 本機的 AD 特權帳號已進行回收，並透過微軟的 Windows LAPS 產出的一次性亂數密碼來進行管理，惟僅限於 PC 本機，不含伺服器、網域等設備。

(四)細分資通訊系統或設備關鍵用途，當資通訊系統依其對營運影響程度、重要程度或資訊敏感程度進行分類，則能依關鍵程度區分網段、設定防火牆規則等，藉以提升網路安全。

二、從駭客攻擊的案例來看，常見的手法是透過現有資通訊產品的程式漏洞，以 Barracuda 為例，該公司所打造的電子郵件安全閘道器(Email Security Gateway，ESG)設備，駭客在 2022 年 10 月就利用其允許遠端駭客注入命令的零時差漏洞植入木馬，然該公司在 2023 年 5 月 19 日才發現該漏洞，同年 20 日及 21 日便修補所有的 ESG 設備，並已通知受影響的用戶，也提醒該公司的調查僅限於 ESG 設備本身，而非用戶的環境，遭到入侵或攻擊的用戶應該檢查自己的環境以判斷是否必須採取其它行動。公司目前對於現有資通訊產品的程式漏洞，建議採取行動如下：

(一)集中管理公司的資通訊產品，目前資訊單位已使用 WinMatrix 進行管理，可回報數量及用來確認軟體更新狀態，惟少部分非屬資訊單位管轄的資通訊產品則自行管理軟體更新及漏洞修補，亦即無法得知及確保漏洞修補數量的完整性。

(二)修補資通安全弱點通報系統(VANS)回報的弱點項目，尤其是高風險指數的項目。

(三)對新增或異動的應用程式於上線至正式環境前進行源碼掃描，雖然公司無法像 Microsoft 對開發人員在開發過程中新增的應用程式進行掃描，建議可在正式上線前進行掃描並且修補弱點。

三、當企業員工的資安意識不足時，就容易成為破口，尤其利用社交工程駭入的方式，通常是最快速而且最不花費成本的方式，目前公司在提升資

通安全意識的作法主要為資安宣導、資安教育訓練及社交工程演練，建議未來可考量的方向如下：

(一)對於自行辦理的社交工程演練，不要預告演練期間，才能有效提升資安意識。

(二)鼓勵通報的行為，對於有效通報應給予獎勵，當員工看到什麼就說什麼，代表員工隨時保持在警戒狀態。

(三)在資安宣導方面，減少將資安相關內容密集條列後一次性傳遞，可拆分內容主題，需簡明易懂且少量訊息，員工較能吸收且增加注意力，始能達到資安宣導目的。