BCCS 漢昕科技

長庚學校財團法人長庚科技大學
一般人員教育訓練

莊瑞倫 Allen Chunag

本次教育訓練的目的?

- 對資訊安全應有之認知
- 瞭解各項資訊安全攻擊態樣和預防
- 瞭解資訊安全威脅與重要性，及其保護的方法，期能有效地配合政策之施行

- 何謂資訊安全？
- 近期國內資安事件案例分享
- 常見的攻擊手法
- 資訊安全防護建議
- 常見電腦遭入侵「跡象」與「應對」
- 議題/問題討論

BCCS 漢昕科技

何謂資訊安全？

使用者為什麼成為目標?

- 竊取機密檔案/文件
- 針對性機密資料蒐集
- 線上遊戲、網路購物及網路銀行等服務之有價財產
- 部落格或社群網站之帳號密碼
- 跳板(殭屍電腦)
- 監控使用者行為
- 智慧型手機富含使用者個資(通訊錄、E-Mail等)

何謂資訊安全？

- 一般人員想的是？
- 資訊人員想的是？
- 機關首長想的是？
- 主管機關想的是？
- 攻擊者動機？

何謂資訊安全？

一般人員想的是:

- 可能與個資外洩有關
- 是否因為銀行帳戶外洩被盜領（盜刷）
- 機關內部社交工程信件（演練）
- 日常作業上繁雜的程序

何謂資訊安全？

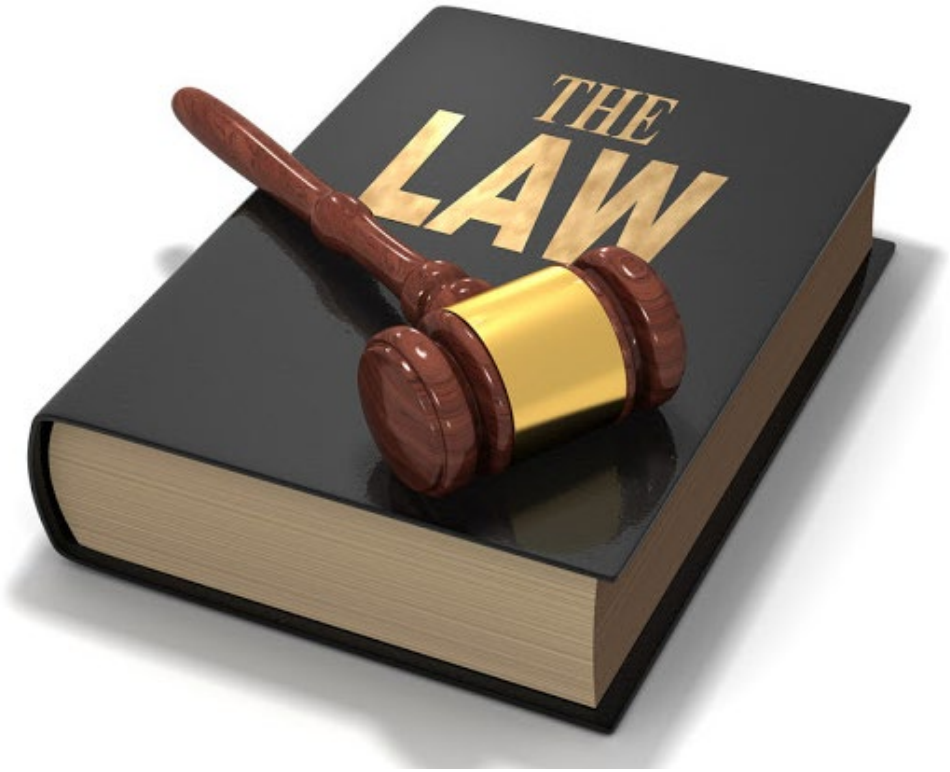
資訊人員想的是:

- 防火牆
- ＶＰＮ
- 入侵預防系統
(Intrusion Prevention System，IPS)
- 入侵檢測系統
(Intrusion-detection system，IDS)
- 防毒軟體
- 認證授權管理
- 帳號管理
- 日常作業上麻煩的程序！

何謂資訊安全？

機關首長想的是:

- 機關內重要資訊不被篡改、不被洩漏、未經授權不可使用。
- 通過 上級機關/驗證公司 稽核。
- 符合相關法規要求。
- 以精簡的經費符合上述所有要求。



何謂資訊安全？

主管機關想的是:

- 確保國防、外交或國土安全。
- 避免公務機關功能受影響、失效或中斷。
- 避免個人機密、公務機密或其他資訊遭未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害。
- 關鍵基礎設施運作正常（能源、水資源、通訊傳播、交通、銀行與金融、緊急救援醫院）

圖片來源：freepik，CC Licensed。

何謂資訊安全？

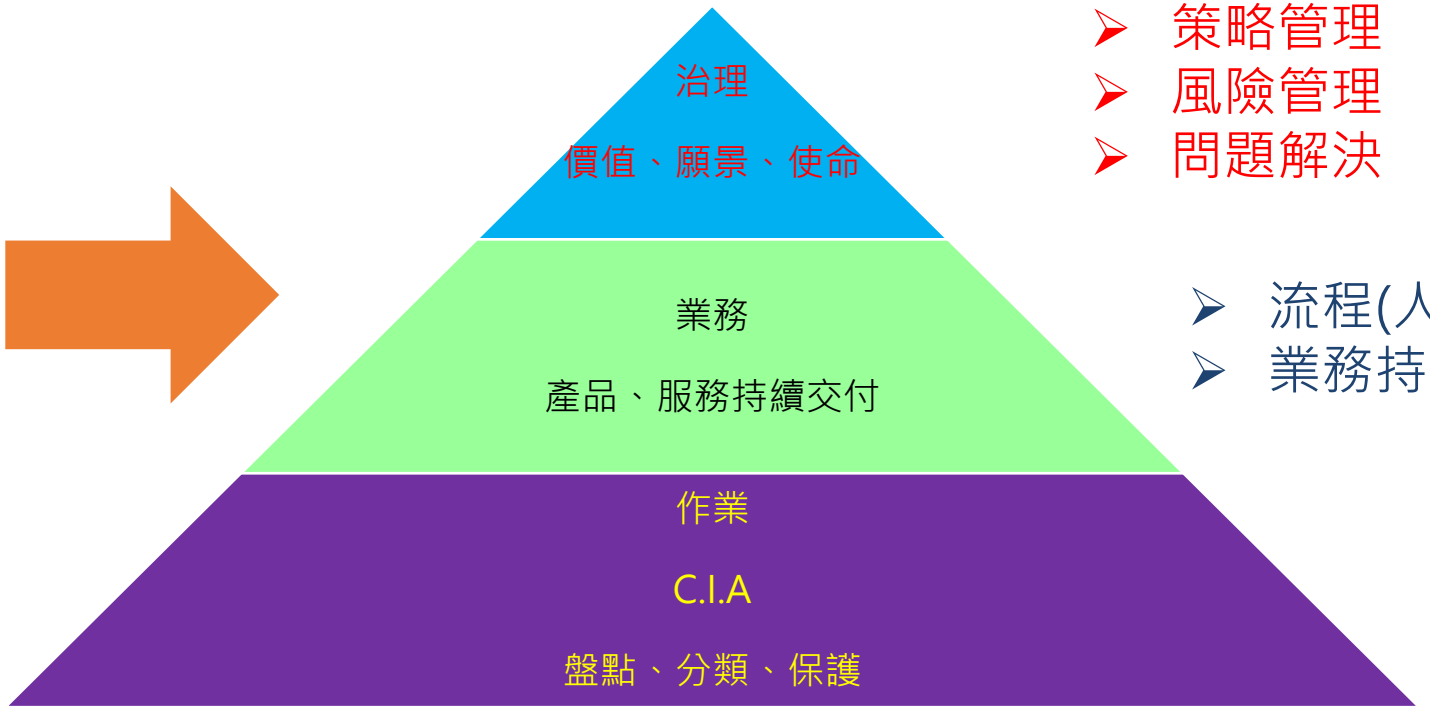
攻擊者動機:

- 認知作戰
- 竊取情資、網路間諜
- 個人、商業利益
- 報復行動
- 新手練功

何謂資訊安全？

資訊安全管理，即是透過安全控制措施保護組織資產，使其免於危害,並達到C.I.A.目標，進而支持組織業務流程確保產品與服務持續交付，並創造價值達成組織願景與使命。**機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）

- ✓ 策略
- ✓ 政策
- ✓ 標準
- ✓ 程序
- ✓ 指引



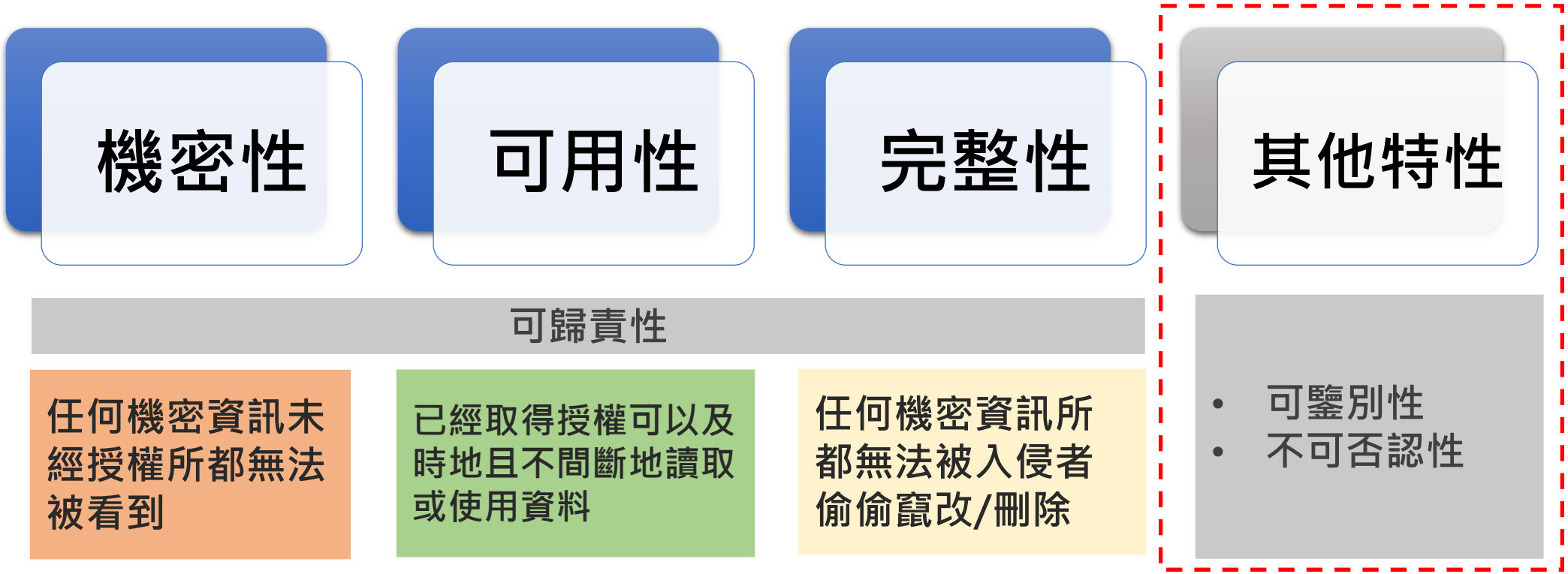
- ➢ 策略管理
- ➢ 風險管理
- ➢ 問題解決

- ➢ 流程(人員、研發、採購、併購)
- ➢ 業務持續營運

- ➢ 盤點、分類、保護
- ➢ 一致性、有效性

何謂資訊安全？

資訊安全三要素:



何謂資訊安全？

	高	中	普
機密性	發生資通安全事件致 資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等 方面將產生非常嚴重或災難性之影響。	發生資通安全事件致 資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機 關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或 災難性之影響	發生資通安全事件致 資通系統受影響時，可能造成對資訊、資通系統之存取或使用 之中斷，對機關之營運、資產或信譽等方 面將產生嚴重之影響。	發生資通安全事件致 資通系統受影響時，可能造成對資訊、資 通系統之存取或使用之中斷，對機關之營運、資產或信譽等方 面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令， 可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之 資通安全相關法令， 可能使資通系統受影 響而導致資通安全事件，或影響他人合法 權益或機關執行業務之公正性及正當性， 並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規 範之情形。

何謂資訊安全？

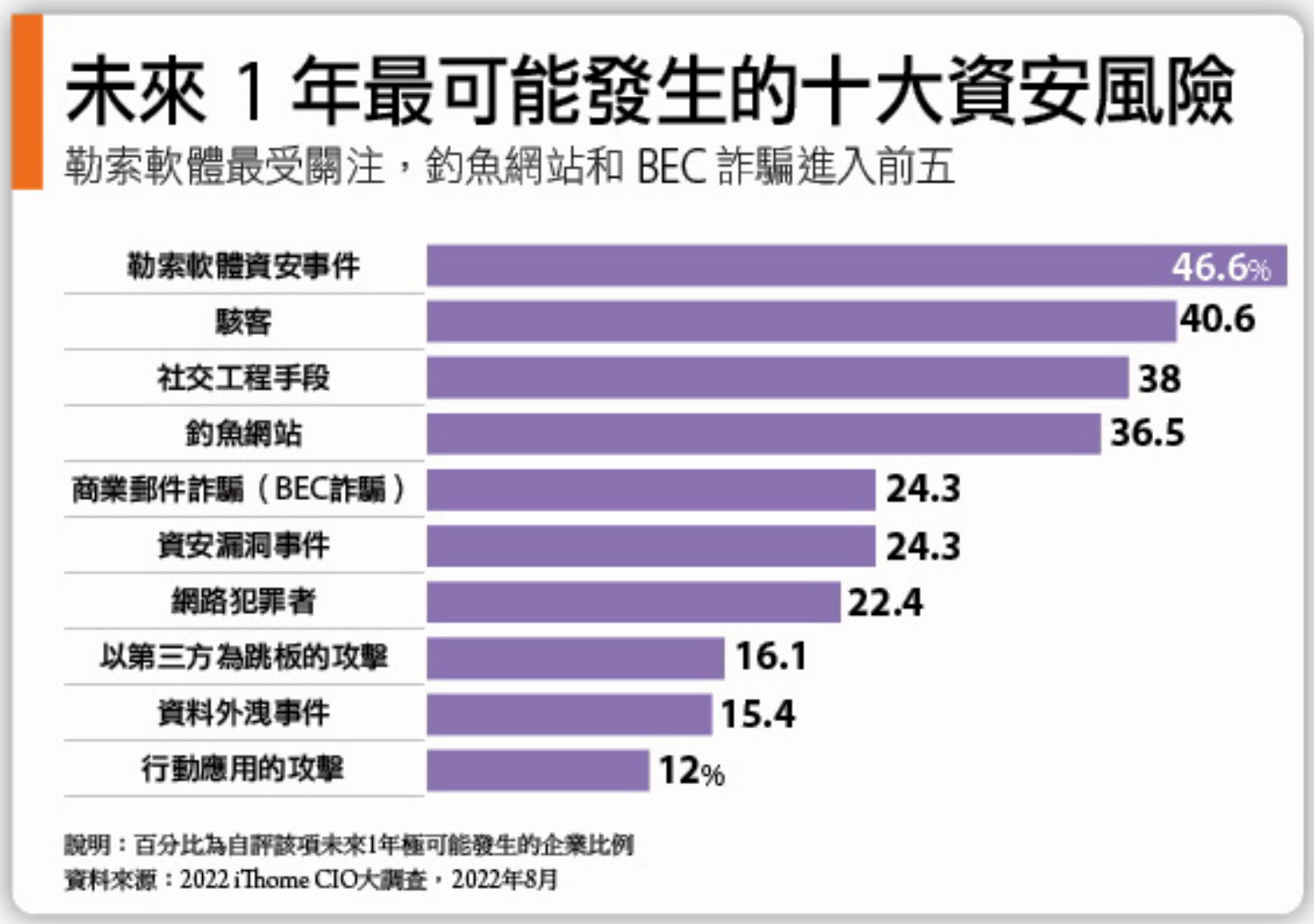
意為保護資訊及資訊系統免受未經授權的進入、使用、披露、破壞、修改、檢視、記錄及銷毀。

政府、軍隊、公司、金融機構、醫院、私人企業積累了大量與員工、顧客、產品、研究、金融資料有關的機密資訊，而絕大部分的資訊現在被收集、產生、儲存在電腦內，並通過網路傳送到別的電腦。

企業的顧客、財政狀況、新產品線的機密資訊落入了其競爭對手的掌握，這種資安性的喪失可能會導致經濟上的損失、法律訴訟甚至該企業的破產。保護機密的資訊是商業上的需求，而在許多情況中也是道德和法律上的需求。
對於個人來說，資訊安全對於個人隱私具有重大的影響，但這在不同的文化中的看法差異很大。

近期國內資安事件案例分享

2022 資安危機


未來 1 年最可能發生的十大資安風險
勒索軟體最受關注，釣魚網站和 BEC 詐騙進入前五
勒索軟體資安事件 46.6%
駭客 40.6
社交工程手段 38
釣魚網站 36.5
商業郵件詐騙（BEC詐騙） 24.3
資安漏洞事件 24.3
網路犯罪者 22.4
以第三方為跳板的攻擊 16.1
資料外洩事件 15.4
行動應用的攻擊 12%
說明：百分比為自評該項未來1年極可能發生的企業比例
資料來源：2022 iThome CIO大調查，2022年8月

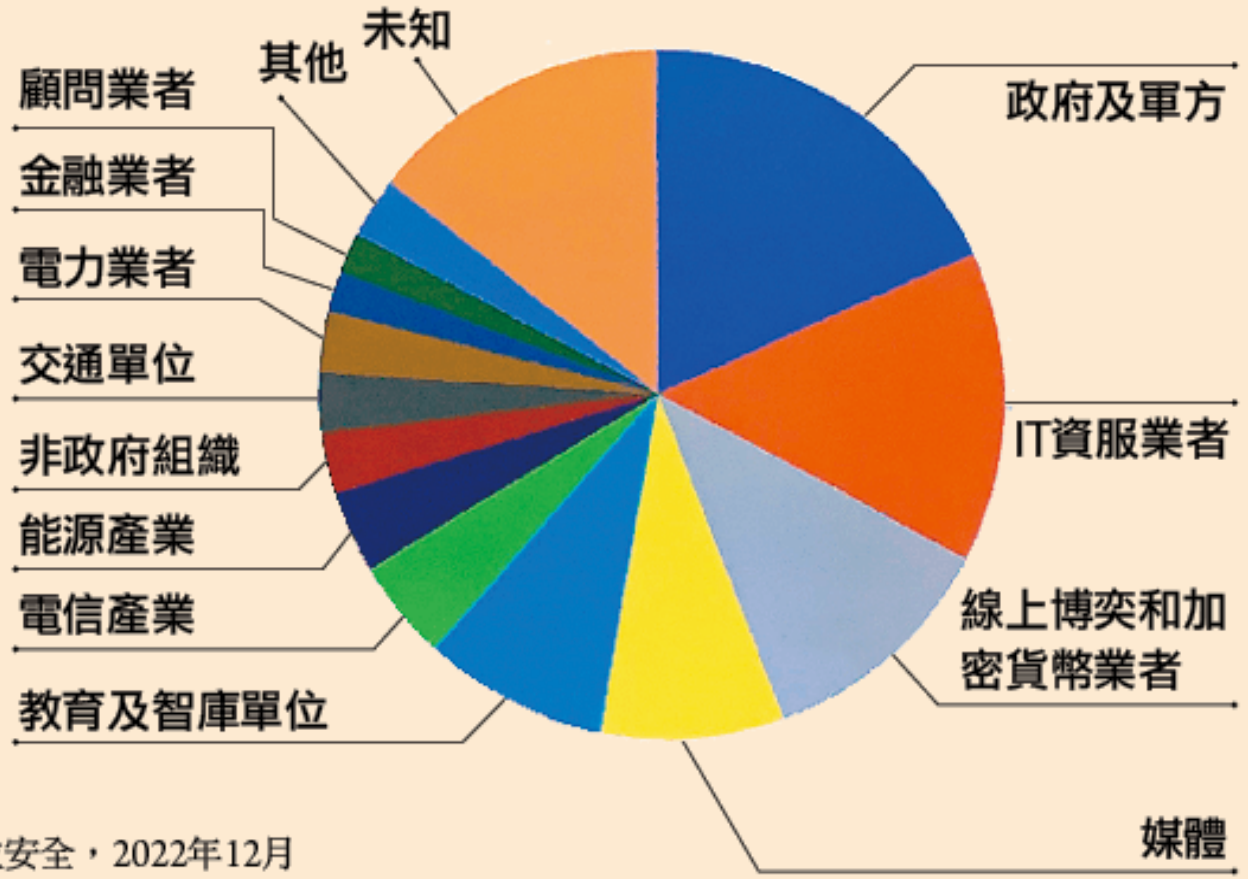
近期國內資安事件

	時間	議題
1	2022年6月	固網電信業者網路服務斷線以致券商及期貨商下單系統異常，12家券商、9家期貨商向證期局通報下單系統無法提供服務
2	2022年8月	美國眾議院議長菲洛西訪台期間伴隨網路攻擊多為網頁竄改、分散式阻斷服務攻擊（DDoS）等等
3	2022年11月	金融業國泰世華銀行因系統升級維護不當，ATM 半年當機四次，受影響帳戶數合計3.5萬戶
4	2022年11月	雄獅旅遊遭受駭客網路攻擊，顧客個資外洩，被不法人士進行詐騙犯罪情事。另外東森購物、誠品、博客來、迪卡儂、旋轉拍賣等眾多業者，也有疑似發生個資外洩事件
5	2022年12月	部立桃園醫院的資訊系統為遭中國大陸網路駭客駭入醫院系統，部桃證實有十二部主機遭駭客入侵。
6	2023年1月	健保署發生公務人員涉嫌外洩健保被保險人個資事件。
7	2023年2月	華航、iRent個資外洩、格上租車訂單資料流出
8	2023年2月	微風集團遭駭 90萬用戶個資外洩

2022年臺灣APT攻擊研究分析

臺灣2022年政府軍方及資服業者受駭比例最高

TeamT5杜浦數位安全技術長李庭閣表示，連續兩年來，政府和軍方是受攻擊主要對象，排名第二的資服業者，主要是被當作駭客攻擊的跳板，可以藉此發動供應鏈攻擊。



資料來源：TeamT5杜浦數位安全，2022年12月

國內資安事件案例分享

- 資料來源
https://ctee.com.tw/news/stocks/669490.html

28日券商下單異常 兇手找到了

工商時報 林淑惠 2022.06.30

針對28日多家券商及資訊業者提供的股市App下單系統出現異常一事，NCC於29日啟動行政訪查後表示，是中華電信為了保護網路避免受到攻擊啟動了保護機制。圖／freepik

針對28日多家券商及資訊業者提供的股市App下單系統出現異常一事，NCC於29日啟動行政訪查後表示，不是中華電信或台灣固網設備故障及停電造成，而是中華電信為了保護網路避免受到攻擊啟動了保護機制。

NCC副主委兼發言人翁柏宗表示，中華電信邊界閘道器協定（Border Gateway Protocol，BGP）設有路由筆數上限，因28日BGP監測台灣固網的路由筆數超過了警示上線的六千筆，中華電信才會在9點58分12秒啟動了防護機制，造成台固路由器中斷通訊。

國內資安事件案例分享

- 資料來源
https://www.ithome.com.tw/news/152491

臺灣8月初因裴洛西訪臺而遭到網路攻擊的事件總覽

在美國聯邦眾議院議長裴洛西訪問臺灣的前後，駭客不斷發動攻擊長達超過一週，我們彙整了這段時間發生的資安事故

文/ 周峻佑 | 2022-08-12 發表

讚 78 分享

美國聯邦眾議院議長裴洛西（Nancy Pelosi）於8月2日至3日，率領美國眾議院國會訪問團來臺訪問，此行引發中國政府高度不滿，不只進行軍演，相關的網路攻擊更是從訪臺前就不斷出現，且前後持續了長達9天。這些攻擊手法大致可區分為分散式阻斷服務（DDoS）攻擊、內容置換（Deface），以及幾可亂真的假訊息等。

而在這段期間風聲鶴唳，也有一些公務機關的系統服務出現異常，而被外界懷疑可能也遭到相關攻擊。這些包含了警務系統、司法院法學資料檢索系統、電子發票入口網站等，但都被證實是系統部分元件故障所致。

國內資安事件案例分享

- 資料來源
https://money.udn.com/money/story/5613/6233860

開鍘！國泰世華銀爆四次ATM當機 遭罰增資、禁新設ATM

國泰世華銀行近2年4度出現ATM當機，金管會今對此開罰。圖／國泰世華銀行提供

國泰世華銀從去年10月系統升級後，至今爆發四次ATM、網銀等當機，金管會終於開鍘。

金管會晚間宣布，處國泰世華銀200萬罰鍰外，更祭出五大處置，禁止新設逾200台ATM、究責相關經理人、及要求增提作業資本計提等較重懲處。據金管會估算，國泰世華銀若得維持既有16%高資本適足率，6月底前得增資7.5億元。

這也是繼理專弊案，要求玉山銀也得增提作業風險資本計提後，第二家被要求增提作業風險的資本計提，更是首次被要求禁新設ATM，每一個懲處都是歷年ATM當機事件較重者。

國內資安事件案例分享

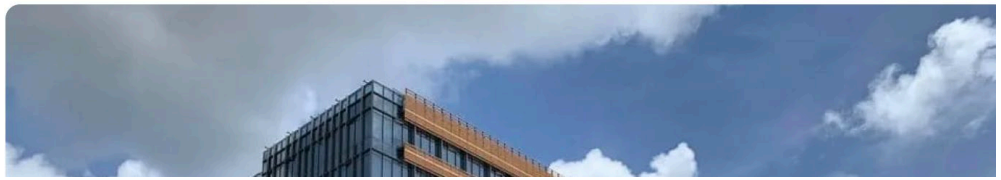
- 資料來源
https://tw.nextapple.com/finance/20221129/ED0F90B7619B481454A69B4521516792

驚傳遭駭客攻擊詐騙消費者！雄獅：已向調查局通報

財經 2022/11/29 16:05

加好友

【記者陳慦蔚／台北報導】雄獅（2731）網路驚傳遭駭客攻擊！公司今表示，駭客惡意攻擊電腦作業系統，並進而向近半年曾於雄獅購買相關旅遊產品的消費者進行詐騙，除已向法務部調查局通報協助外，也以同步委請外部資安公司技術專家共同處理，持續加強資訊安全管理。



雄獅說明，目前從不法人士詐騙手法研判，其不法利用的資料可能包括近半年購買訂房、機票、票券、證照等訂單資料，涵蓋訂單聯絡人姓名、聯絡電話及購買商品內容，但不包括旅客信用卡交易訊息。

雄獅強調，於發現遭駭客攻擊後隨即啟動內部資安相關防禦機制與應變作業，除已向法務部調查局通報協助外，並同步委請外部資安公司技術專家共同處理，並持續加強資訊安全管理。

國內資安事件案例分享

- 資料來源
https://udn.com/news/story/7315/6519354

刑事局公布詐騙高風險賣場 博客來、迪卡儂、誠品上榜

2022-08-07 15:40 聯合報／記者蕭雅娟／台北即時報導

讚 223 分享 分享

刑事局今公布今年第二季受理「解除分期付款」高風險賣場，包含博客來網路書店、迪卡儂、誠品網路書店等。警方指出，歹徒先竊取電商的消費者個資，再陸續假冒客服、金融機構人員，詐騙消費者，前五名民眾通報的高風險賣場均已宣導反詐騙，呼籲民眾慎防詐騙。

詐騙集團使用的話術為「工作人員操作錯誤，導致誤設分期付款、重複扣款或升級成VIP會員，要求客戶前往操作ATM、購買遊戲點數或使用網路銀行、App來解除設定」

警方分析詐騙手法，歹徒首先「駭入」電商或電商委託系統商資料庫，取得消費者個資，包含姓名、電話、消費資料及付款方式；緊接著「偽冒電商業者」客服人員，撥打客服電話給民眾，要求民眾提供消費時的信用卡、金融卡上的金融機構電話號碼。

國內資安事件案例分享

- 資料來源
https://news.ltn.com.tw/news/life/breakingnews/4147163

竊取個資、竄改給藥資料 衛福部桃園醫院遭中國駭客攻陷

桃園醫院被爆採用中國系統，導致資安後門大開。（資料照，本報合成）

2022/12/07 19:10

〔記者鄭淑婷／桃園報導〕衛福部桃園醫院資訊系統被爆採用中國系統，從2020年8月起陸續發生遭駭客入侵，竊取病患個資、醫護資料，植入惡意程式等，更出現醫療錯誤資訊，危害到病患安全，桃園醫院早於2020年2月即與系統商昱誠智能服務股份有限公司結束合約，但目前仍採用這套系統，只是改由自行維管，全案已報請警方、調查局偵辦中；桃園醫院今天發布聲明指出，前年確實有發現駭客入侵事件，但僅有1台主機遭受影響，主機內無個資，並無病人個資外洩疑慮，至今也無任何個資外洩情事，非如爆料內容所言。

國內資安事件案例分享

• 資料來源
https://news.ltn.com.tw/news/society/breakingnews/4180017

健保署3人被控查洩個資13年 疑涉國家情報工作

衛生福利部中央健康保險署傳出健保被保險人個資外洩案，檢調兵分多路搜索及約談，9日晚間將已退休的健保署前主秘葉逢明移送台北地檢署複訊後，以被告身分暫獲請回。（記者羅沛德攝）

2023/01/10 06:51

〔記者錢利忠／台北報導〕衛生福利部中央健康保險署驚傳有「內鬼」外洩民眾個資！已退休的健保署前主秘葉逢明、在職的健保署承保組科長謝玉蓮、承保組職員李仁輝等3人，被健保署內部職員檢舉，涉嫌從內部系統偷查民眾的健保個資；台北地檢署指揮調查局新北市調查處兵分5路搜索健保署及3被告住處，原依可處3年以下徒刑之刑法洩漏或交付國防以外機密罪偵辦；不過，謝女於今凌晨4時許訊後，被改依違反「國家情報工作法」諭令10萬元交保，案情急速升溫。

據了解，謝女被檢調查出，她偷查的健保個資被害人中，疑似包含了警察、調查官、移民署官員等可能涉及國家情報工作法所規範的「情報機關人員」，因而涉及「刺探或收集」國家情報資訊等罪嫌，不過尚缺乏洩漏或交付給包括中國在內等敵對勢力的事證，暫時僅止於「偷查」，才諭令她10萬元交保。

國內資安事件案例分享

- 資料來源
https://www.businesstoday.com.tw/article/category/183027/post/202302150040/

從華航到iRent都被「駭」 資安危機事件一演再演.....
40天四起個資外洩 中小企業資安拉警報

成立邁入第9年、已奪下台灣共享租車龍頭的iRent，日前意外爆出40萬消費者個資遭洩，公路總局依《個資法》開罰20萬元。

月底，和泰集團旗下共享汽車品牌iRent，被爆出四十萬名消費者的個資遭外洩，舉凡消費者的姓名、手機號碼、身分證、住家地址、駕照照片，通通被駭客揭露。iRent後續聲明表示，由於暫存資料庫沒有完整阻擋外部連線，導致被駭客使用特定工具及技巧進入。

然而，這已是今年僅過不到兩個月以來，第四起個資外洩。一月中，掌握台灣兩千三百萬人健康資料的健保署，爆發官員盜賣民眾個資；同一個禮拜，華航也被踢爆會員資料外流，包括副總統賴清德、名模林志玲的個資都外洩，二月上旬，格上租車也發生訂單資料流出。

國內資安事件案例分享・資料來源https://udn.com/news/story/123309/6989196

udn / 產經 / 強化資安

微風遭駭 90萬用戶個資外洩

2023-02-23 00:48 經濟日報／記者林海、馬瑞璿、何秀玲／台北報導

+ 資安

日前有人在駭客論壇聲稱竊得微風百貨的內部資料，微風表示，近日收到匿名網路勒索信件，第一時間立即啟動損害機制，目前內部資安團隊已完成軟體及作業系統安全性更新。記者曾學仁／攝影

微風集團遭駭概況

事發經過	有人在駭客論壇BreachForums聲稱，竊得微風百貨內部資料
微風因應措施	1.近日收到匿名網路勒索信件，第一時間啓動損害機制 2.目前內部資安團隊已完成軟體以及作業系統安全性更新，同時提高資安防護層 3.經內部清查確認，外流個資與公司資料庫有所落差，因此駭客未必是從微風駭入

資料來源：採訪整理　　何秀玲／製表

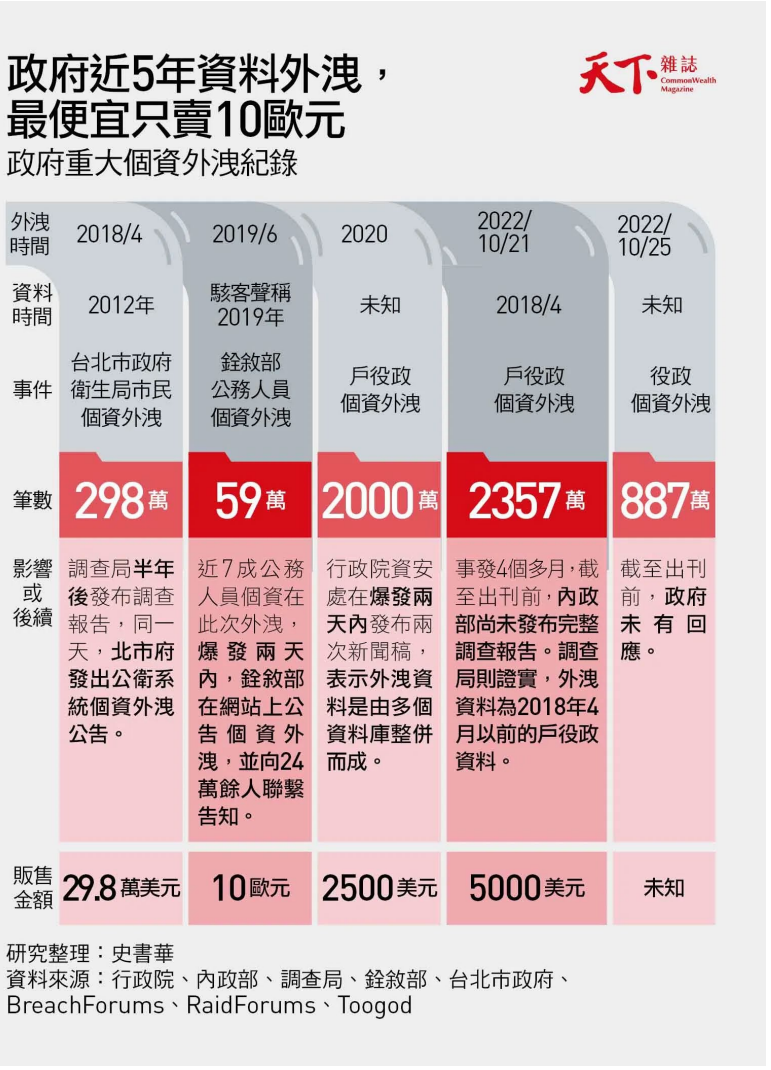
圖／經濟日報提供

BCCS 漢昕科技

國內資安事件案例分享

2022年10月21日，以「OKE」為代號的匿名使用者，在駭客論壇BreachForums兜售號稱全台2300萬筆戶役政資料。為了吸引顧客買單，OKE更直接公開20萬筆設籍在宜蘭的個資當作商品樣本。

其中包含39個欄位，從個人生日、性別、身分證號等資訊外，戶號、戶長，甚至是生父生母、養父養母都有單獨欄位和對應的身分證號。

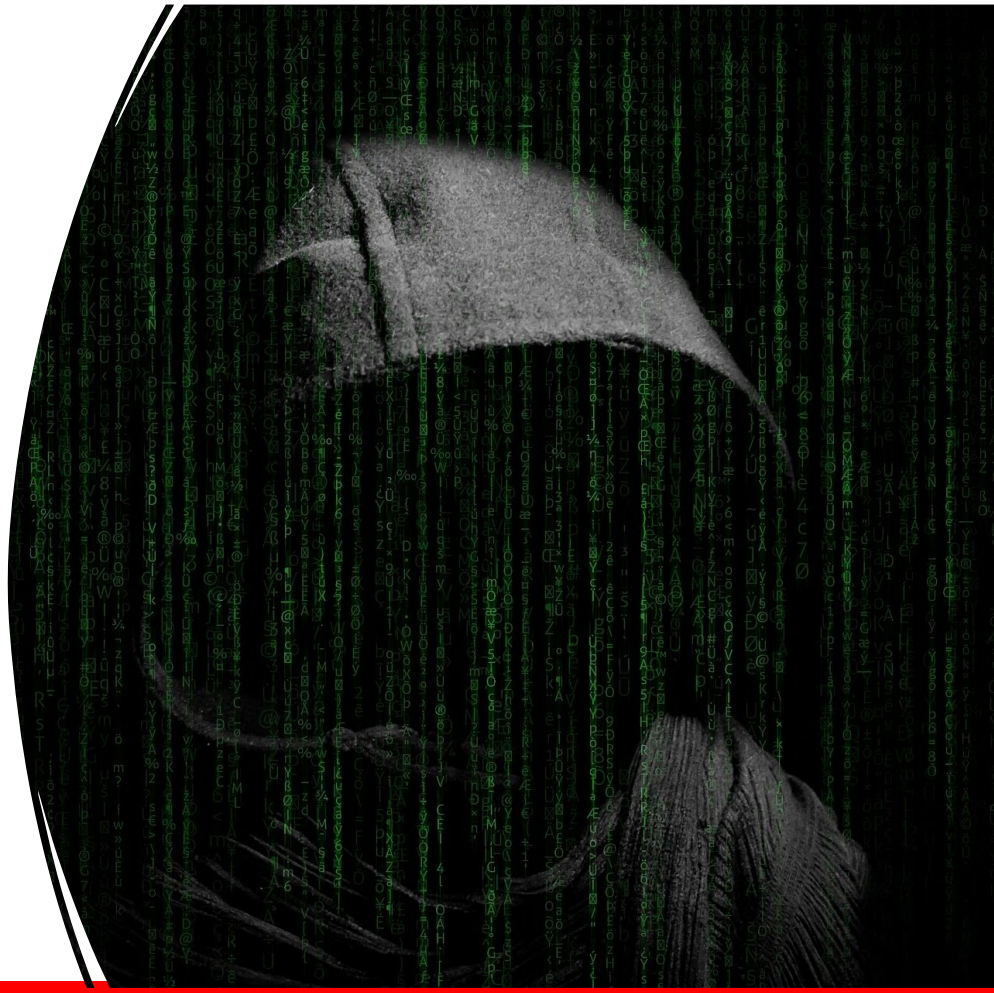


常見的攻擊手法

何謂資訊安全？

實際上駭客常用手法:

- 文件中夾帶惡意巨集病毒
- Cookie竊取
- 物聯網攻擊
- 分散式阻斷服務攻擊（DDoS）
- 網路釣魚（Phishing）
- 點擊劫持（Clickjacking）/ 介面偽裝（UI redress）
- 中間人攻擊（Man-in-the-middle attack）
- 跨網站指令碼攻擊（Cross-site scripting，XSS）
- DNS 欺騙（DNS spoofing）
- 水坑攻擊（Watering hole）
- 鍵盤側錄器攻擊（Keylogging）
- 暴力攻擊（Brute force）/字典攻擊
- 社交工程
- 進階持續性滲透攻擊（Advanced Persistent Threat, APT）



常見的攻擊？

文件中夾帶惡意巨集病毒:

- 文件中隱藏的惡意巨集是一般人不會特別注意的惡意軟體，但其實這種惡意病毒很容易察覺。Excel 或 Word 等文件都能製作巨集，打開文件後能執行巨集中的指令碼，但通常打開文件時，會提示需要用戶授權才能使用巨集功能。如果您允許文件執行巨集，巨集中的指令碼可以在系統中打開許多漏洞，讓駭客上傳更嚴重的惡意軟體來控制您的電腦。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

Cookie竊取:

- Cookie 不僅是廣告商追蹤用戶行為的方法，也是網站追蹤用戶登入登出活動的方法，當您登入帳戶時，網站會發送一個 Cookie，讓網站能記住用戶的登入行為。但如果經由不安全的連線發送 Cookie，這個 Cookie 可能會被駭客竊取甚至竄改。

- Cookie 竊取就是駭客利用不安全的連線竊取用戶的 Cookie，並在網站上假扮您的身份，他們可能無法取得用戶的登入資訊，但可以更改一些設定來劫持已登入的帳戶，進而執行進一步的攻擊。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

物聯網攻擊:

- 物聯網設備（IoT）讓人們的日常生活充滿更多的可能性。不過

物聯網設備也非常容易受到駭客攻擊，這些設備的運算能力和儲存空間有限，在廠商專注於功能的情況下，往往忽略了設備的安全性。而且用戶通常不會修改物聯網設備的密碼，導致設備的預設密碼仍然有效，這表示幾乎任何人都能登入。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

Hacking Gogoro

車鑰匙 Security_Key 🔑

- ECU_Response =SHA256(ECU_Challenge, **Security_Key**)
- 早期版本 Security_Key 就放在 Document 目錄下(有稍微加密)
  - iOS MobileAppProp.plist 中 ScooterSKey
  - Android Settings.xml 中 AppSettings_DefScooter/encryptedkey2
  - 解密方式法 AES-256, CBC/PKCS7Padding, IV=UserId, Key = ScooterUUID
- iTunes 或 Android 備份程式預設會拷走
  - 插上傳輸線 Juicy Attack、從 PC iTunes 備份、各種方式
  - AndroidManifest.xml 中 allowBackup 目前是 true
- 從 WebAPI 取得
  - Try 出 My Gogoro 密碼 (帳單、論壇、App)
  - 偷出 Cookie (Web_Token 也存在 MobileAppProp.plist)
  - https://mobile-pro.gogoroapp.com/WebService/Web/GetKey

Insecure App Data Storage

- Token, Certificate 應該放在加密儲存區
  - 未使用中 是加密狀態、使用中 管制 Timeout
  - 限制 user、限制 process、限制 export

Gogoro電動機車車主能綁定手機發動，卻被點出系統漏洞，駭進程式取得資料後，第二隻手機也能遙控。

主講者：「車子連上了，我按下發動按鈕，車子就發動了。」

▲會議上點出了Gogoro的系統漏洞。

就是台灣駭客協會成員，但他們不是惡意攻擊，而是要幫企業揪出資安漏洞。

資料來源:HITCON

常見的攻擊？

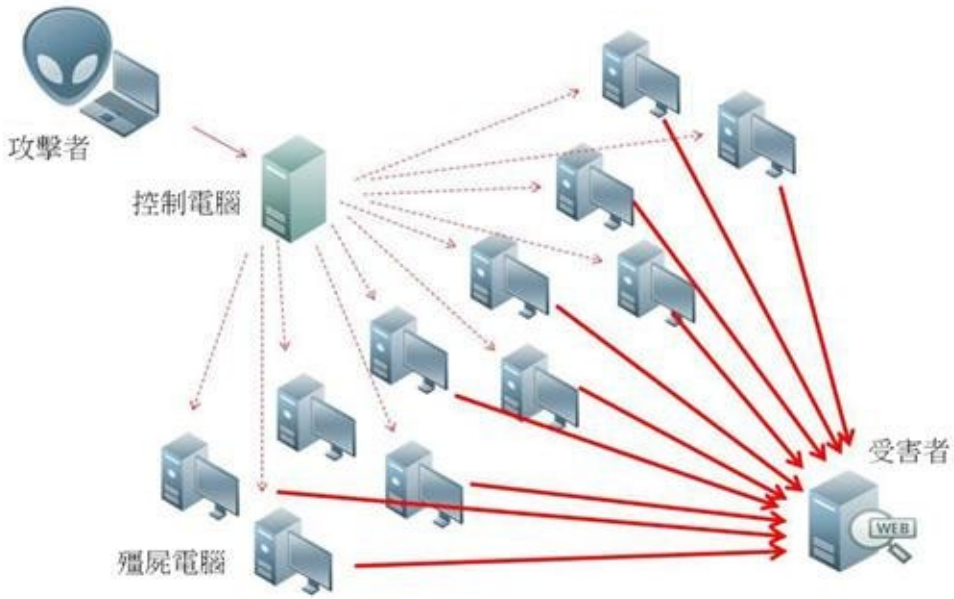
Hacking Tesla

Stole a Tesla

常見的攻擊？

分散式阻斷服務攻擊（DDoS）：

- 分散式阻斷服務攻擊又稱DDoS攻擊，這是一種常見的網路攻擊手法。執行這些攻擊的惡意程式不會傷害受感染的設備，而是將這些設備組成殭屍網路，在短時間內發動大規模的攻擊，藉此耗盡資源和頻寬，造成服務癱瘓。駭客可以透過惡意程式或網站感染許多設備，並控制這些設備向目標網站發送大量請求，導致目標網站不堪負荷而中斷服務。



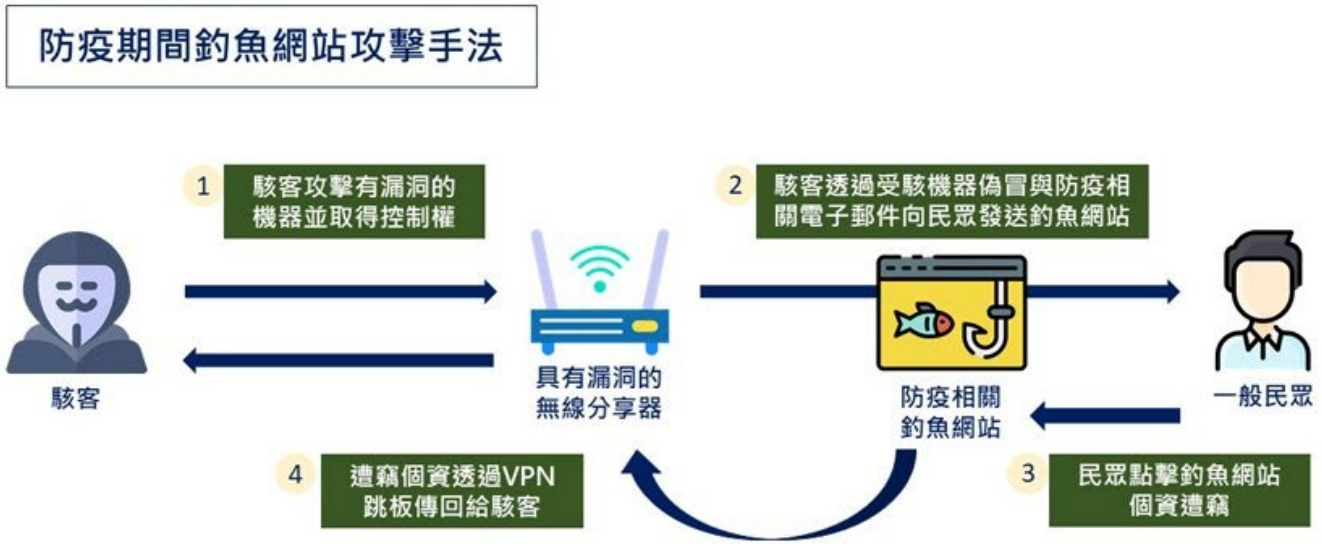
圖片來源:凌群電子報

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

網路釣魚（Phishing）：

- 與大多數駭客攻擊不同，網路釣魚的目標是設備的用戶，而不是設備本身。這種攻擊經由一封精心設計的電子郵件來欺騙受害者，誘導受害者打開郵件上的惡意網站連結或郵件上的附件，讓受害者的設備受到感染，進而竊取設備上的機密資訊。



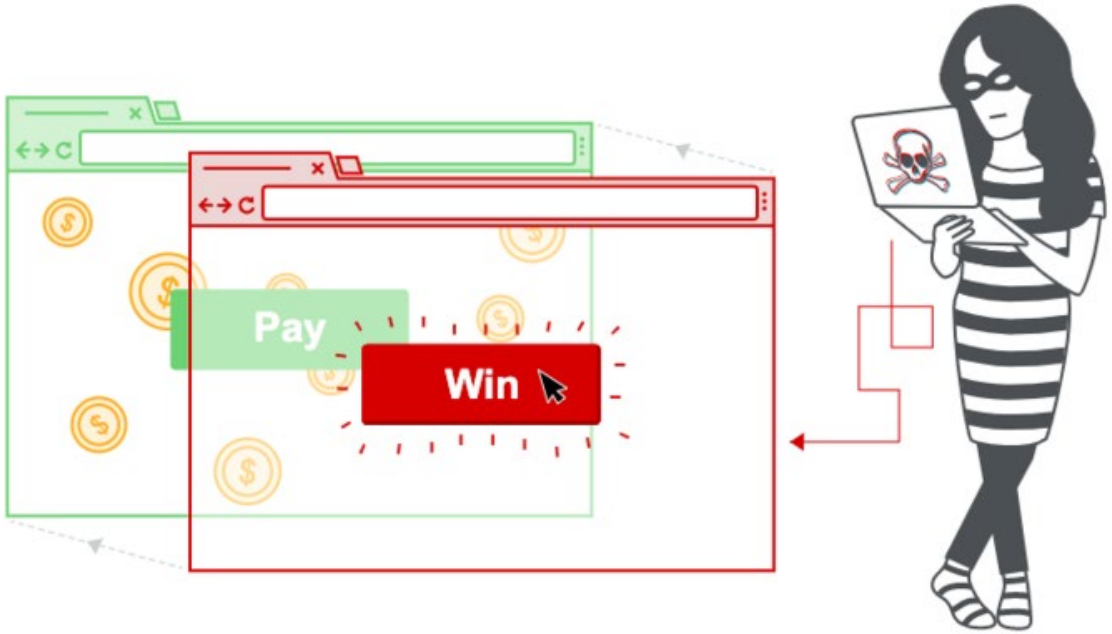
圖片來源:刑事警察局

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

點擊劫持（Clickjacking）/ 介面偽裝（UI redress）：

- 許多用戶可能在瀏覽網站時，沒有注意到它其實是惡意網站，或者是合法網站被入侵後成為惡意網站。這些網站看似正常的網頁上，隱藏著看不見的框架或按鈕，引誘用戶點擊或誤觸，有些攻擊甚至可以追蹤用戶的滑鼠和鍵盤行為。用戶執行的任何一次點擊都是在執行某種他們不知道的動作。



資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

中間人攻擊（Man-in-the-middle attack ）：

- 中間人攻擊（ MITM）又稱為竊聽攻擊，攻擊者在用戶和網站之間，將自己作為一個隱形的中間人。一但攻擊者攔截流量，就能監控並竊取資料，甚至可以在不被察覺的情況下竄改內容。

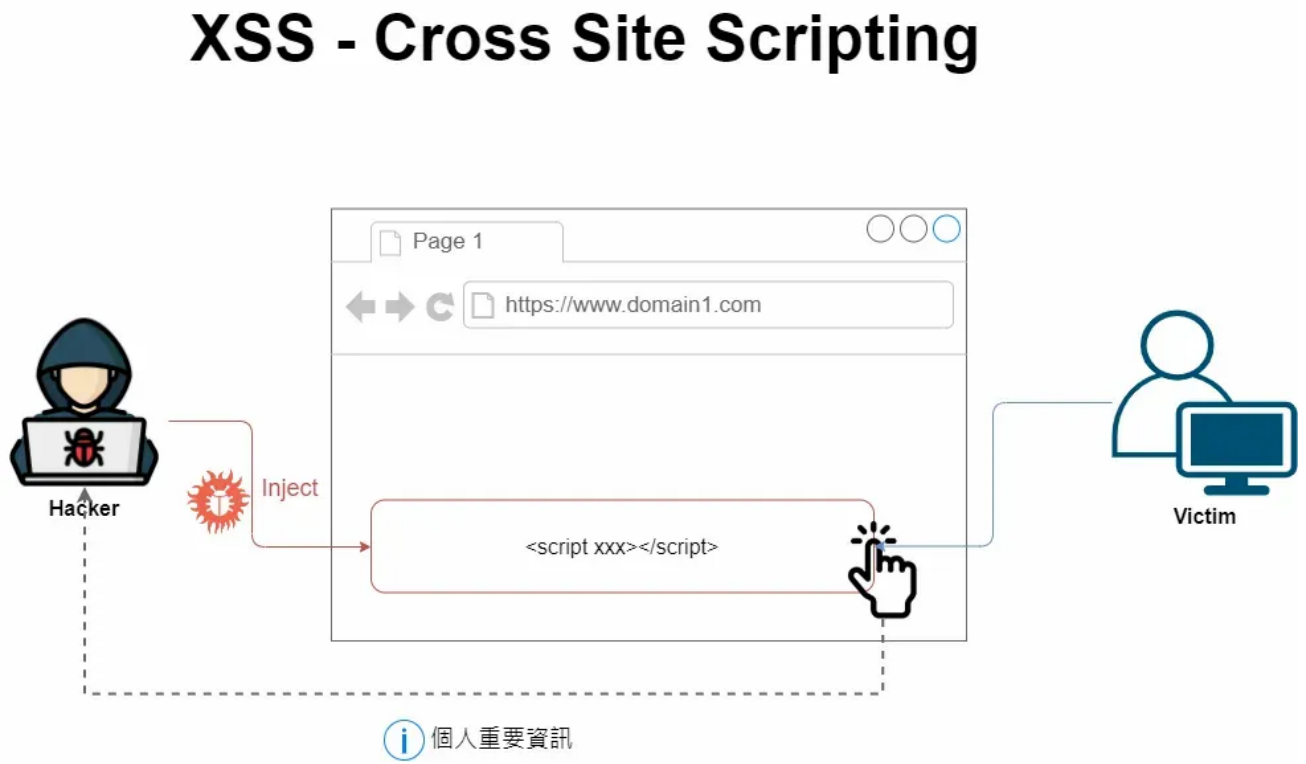
- 中間人攻擊有很多不同的手法，最常見的方法是引誘受害者連上駭客自己的 Wi-Fi 熱點或入侵公用 Wi-Fi 熱點（假冒無線熱點攻擊），就能輕鬆扮演中間人角色，竊取受害者的機密資料。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

跨網站指令碼攻擊（XSS）：

- 網站通常會連結不同的服務以強化各種功能。例如不必每次交換資料時都要重新進行身份驗證。這些連結可能包括廣告服務或特殊插件。
- 如果網站中的某個連結被駭客入侵，攻擊者可以將惡意程式碼直接注入到網頁上，進而讓瀏覽網站的用戶受到影響。這些程式碼可以竊取用戶登入網站的資訊，或者執行不同類型的攻擊，例如點擊挾持。

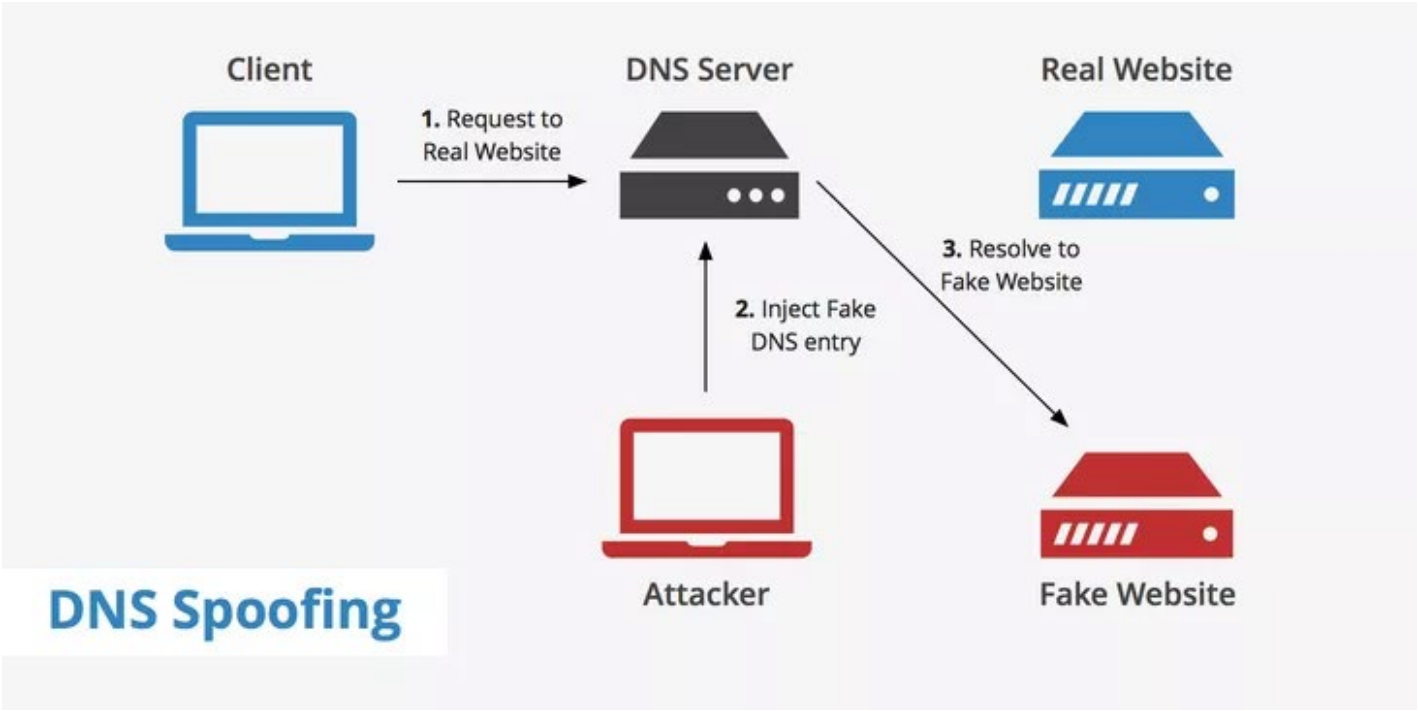


資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

DNS 欺騙（DNS spoofing）：

- DNS欺騙是指攻擊者冒充功能變數名稱伺服器的一種欺騙行為。攻擊者通過入侵DNS伺服器、控制路由器等方法把受害者要訪問的目標機器功能變數名稱對應的IP解析為攻擊者所控制的機器，這樣受害者原本要發送給目標機器的數據就發到了攻擊者的機器上，這時攻擊者就可以監聽甚至修改數據，從而收集到大量的信息。
- 例如讓DNS伺服器解析銀行網站的IP為自己機器IP，同時在自己機器上偽造銀行登錄頁面，那麼受害者的真實賬號和密碼就暴露給入侵者了。



圖片來源:iT邦幫忙

資料來源https://wiki.mbalib.com/zh-tw/DNS%E6%AC%BA%E9%AA%97

常見的攻擊？

水坑攻擊（Watering hole ）：

什麼是水坑式攻擊呢？水坑式攻擊是一種網路攻擊的策略。當攻擊者想要攻擊特定族群（組織、公司、地區）時，攻擊的流程會分成三個階段。
1. 先觀察或猜測特定族群使用的網站。
2. 利用惡意程式嘗試入侵這些網站。
3. 最後當特定群組的成員來瀏覽這些被入侵的網站時就會被感染。

就像非洲的大草原上，獅子在水池附近等待來喝水的動物一樣。駭客會先觀察攻擊目標習慣瀏覽那些網站，鎖定這些網站後開始入侵並植入惡意程式。等攻擊目標瀏覽該網站就有可能被感染。

資料來源https://scitechvista.nat.gov.tw/Article/c000003/detail?ID=1ff276c2-e39b-4f31-a2f8-a5d1872c95bb

常見的攻擊？

鍵盤側錄器攻擊（Keylogging）：

- 鍵盤側錄器會秘密擷取鍵盤上敲擊的按鍵，受害者不會察覺打字內容被側錄。窺探者透過鍵盤側錄器、軟體或硬體記錄用戶輸入的數據來完成這項工作。然後，就可以輕易竊取密碼和其他機密資料。

- 雖然鍵盤側錄器本身並不違法，但駭客卻能將其用於非法目的。

常見的攻擊？

暴力攻擊（Brute force）：

- 在暴力攻擊中，駭客嘗試猜測密碼、PIN 碼或加密金鑰。駭客透過這種攻擊手法，可以存取受保護的服務和資料庫，或者解密資料。

- 駭客使用的軟體每秒會嘗試大量密碼組合，直到猜測正確密碼為止。因此，如果您的密碼規則很簡單，這類軟體只要幾秒就能破解密碼。然而，破解複雜密碼則需要幾年的時間。

- **如果駭客的程式每秒可以嘗試 1000 組密碼，破解一個內含大小寫、數字與符號的 11 字元的密碼僅需 3 天，破解另一個 20 字元的密碼卻得花上數百年。**

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

字典攻擊:

- 字典攻擊是一種暴力攻擊手法。不同之處在於字典攻擊，駭客使用預定義的密碼清單。字典中有時包含常用的密碼短語，有時可能包含所有字典條目。

- 駭客在編輯詞典時通常會進行敏銳的研究。他們可以分析用戶的社群媒體檔案和其他公開可用的資料，找出寵物、親戚和興趣的名字，讓字典更準確。基本上，字典攻擊是暴力攻擊更具自訂性和針對性的變體。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

社交工程(1/3):

- 社交工程 (Social Engineering) 係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破個人、企業或政府機關的資通安全防護，遂行其非法的存取、破壞行為。

常見的攻擊？

社交工程(2/3):

- 社交工程 (Social Engineering) 係**利用人性弱點**，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破個人、企業或政府機關的資通安全防護，遂行其非法的存取、破壞行為。

- 社交工程攻擊(Social Engineer)過程重現

影片觀賞-https://youtu.be/8DqE21SBHl0

常見的攻擊？

社交工程(3/3):

- 常見的社交工程攻擊方式如下：
  1.利用電話佯裝資訊人員，騙取帳號及通行碼。
  2.偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。
  3.利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。
  4.利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。
  5.利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式、p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料。
  6.利用通訊軟體，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

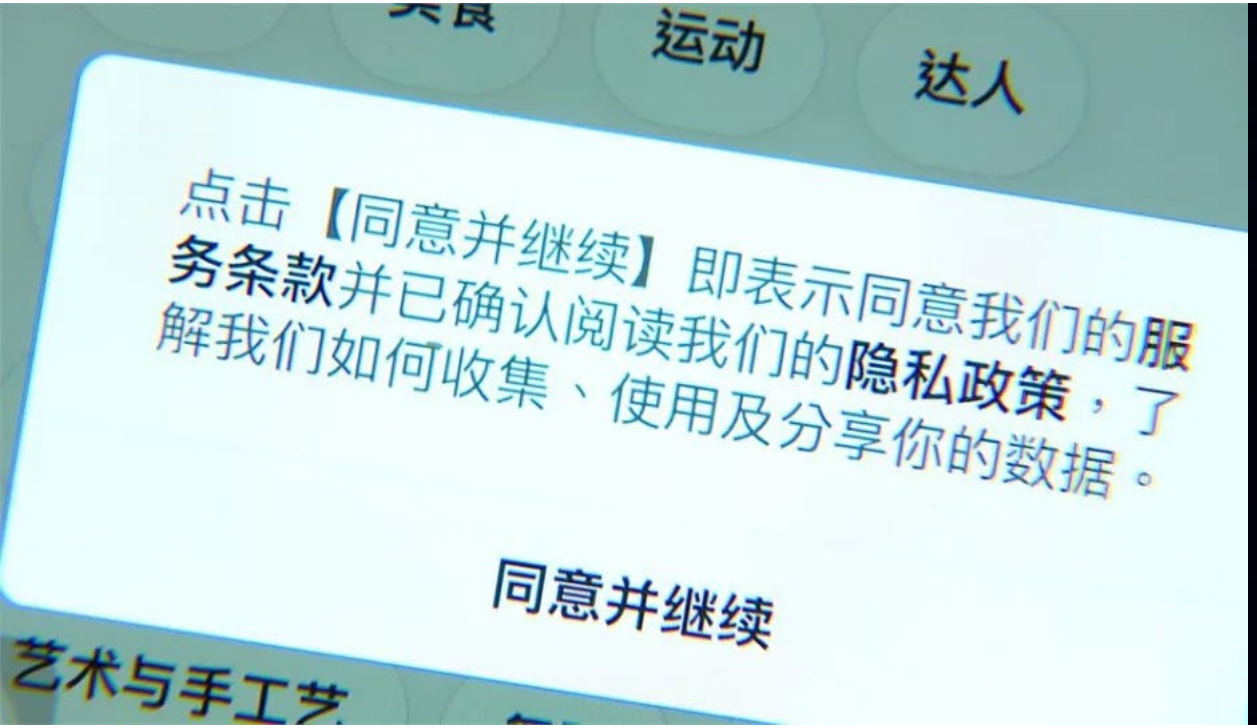
APT攻擊:

- 簡單的說就是針對特定組織所作的複雜且多方位的網路攻擊。APT 進階持續性滲透攻擊(Advanced Persistent Threat, APT)可能持續幾天， 幾週， 幾個月， 甚至更長的時間。APT攻擊可以從蒐集情報開始， 這可能會持續一段時間。它可能包含技術和人員情報蒐集。情報收集工作可以塑造出後期的攻擊， 這可能很快速或持續一段時間

- (APT攻擊:一場沒有中立國的戰爭(真實案例模擬))

影片觀賞-https://www.youtube.com/watch?v=RyQiz8AudQo

新型資安漏洞？



當你點選同意，就等同你可能把所有的數據讓APP取用

新型資安漏洞？

雲端儲存有其難以克服的資訊安全缺點，畢竟實務上根本沒有所謂「絕對的安全」。雲端儲存雖然方便，但其所帶來的侵害隱私或資料竊取的危害，有時甚至大於其使用的便利性

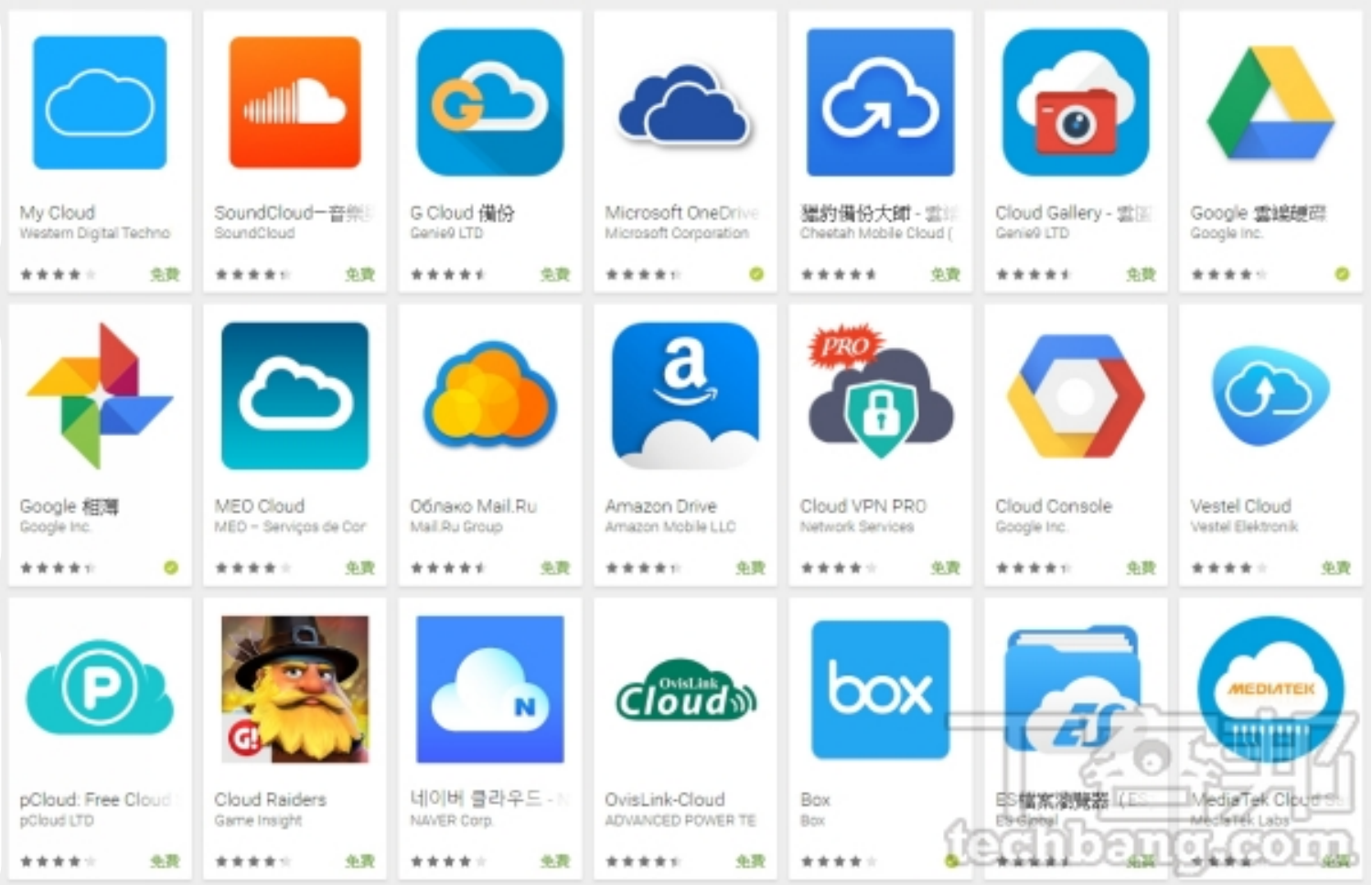
圖片來源:T客邦

新型資安漏洞？

將組織資料存放至雲端之中，USER真的清楚知道服務供應商是如何保護這些資料的？採取了哪些安全控制？有哪些資料是被允許可以存放上雲端的？

在組織之中，會依照職務角色設立不同的資料存取權限，以確保資料的安全，雲端上任意分享組織的檔案，是獲得授權的嗎?

人員離職時，這些存於私人帳戶中的的機敏資料，是要怎麼強制抹除或移交?



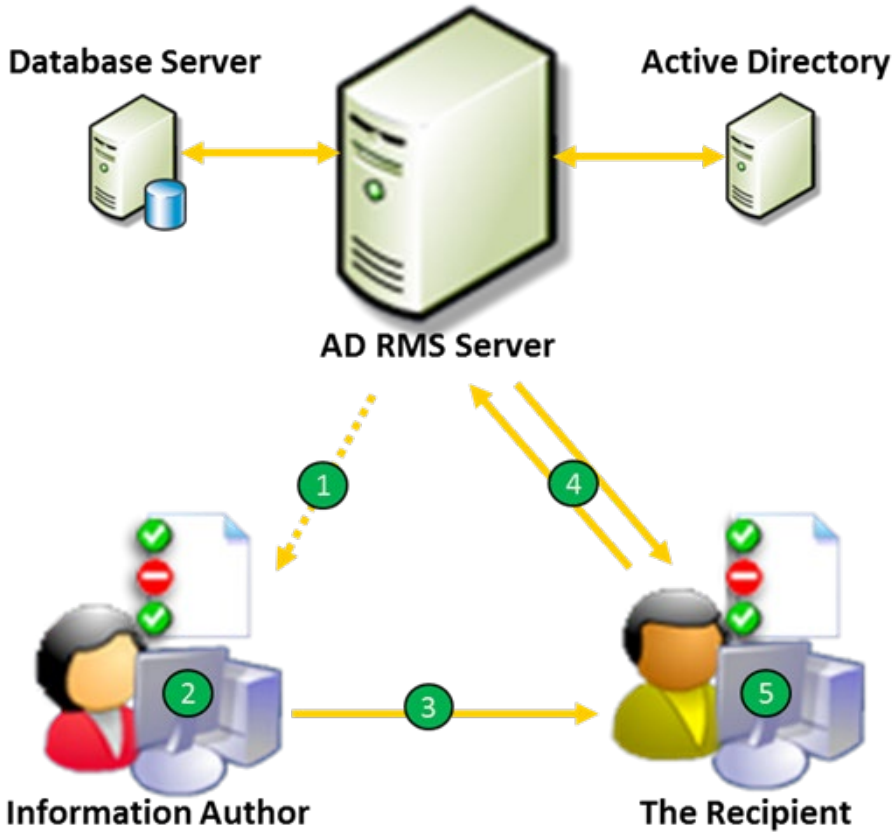
新型資安漏洞？

建議可採取之相關措施

1. 從公司網路上和電腦上封鎖對雲端硬碟的存取，取而代之的是配置公司正式提供的公有雲端硬碟平台。(ex:M365 OneDrive、G suite 雲端硬碟、內部File Sharing主機)

2. 公司內機密資料經過特殊加密(Ex: Active Directory Rights Management Service ，AD RMS)，使其即便外流也無權存取。

3. NDA切結書增列雲端硬碟，從法務面約束。



BCCS 漢昕科技

資訊安全防護建議

即時通訊軟體注意事項(1/2)

- 不得於公務個人電腦安裝
- 以傳送溝通訊息為主
- 傳遞訊息，內容不得涉及機密性、安全性、隱私性或洩漏個人資料
- 機關聯絡群組，指定管理人員
- 管理人員應建立群組名冊並定期清查群組成員，每月將群組訊息內容

即時通訊軟體注意事項(2/2)

- 機關交付正式文書，應循現有行政程序辦理(例如:公文、E-mail)
- 管理員應適時向群組成員宣達使用注意事項，發現問題應立即處理。成立群組目的消失，應即時刪除。
- 群組成員發現誤傳或內容不當者，應即時主動通報管理員處置

電腦安全

- 長時間離開辦公室，記得將電腦關機
  - 杜絕來自網路破壞
  - 防止帳號或密碼被盜用
  - 防止重要資料遭竊
- 應用程式不用時，登出應用程式及作業系統
- 離開座位，電腦應該設定螢幕保護程式
- 辦公室電腦不得任意加裝與工作無關之軟體

機密資料保護

- 紙本
  - 機密及敏感文件不可遺留於桌面上，必須存放於安全場所並加以上鎖
  - 作廢、敏感文件不得回收再利用
- 電子資料
  - 重要或敏感檔案要分開存放
  - 設定密碼或以加密軟體保護
  - 建議避免共用資料夾

重要資料備份

- 備份的重要性
  - 預防重要資料或設備損壞遺失
  - 確保可用性
  - 防範勒索病毒
- 可藉由以下方式達到備份目的
  - 不同的儲存媒體
  - 各式各樣的工具軟體
  - Windows本身所提供的程式
  - 網路存放及備份

BCCS 漢昕科技

電腦遭入侵

「跡象」與「應對」

電腦遭入侵「跡象」&「應對」

有些情況下，防毒軟體可能無法偵測到任何威脅，或是無法執行掃描，如果電腦遭到入侵可能會出現以下部分跡象:

1. 您收到勒索軟體訊息
2. 電腦跑很慢
3. 視訊鏡頭自行開啟
4. 您的朋友收到來自您電子信箱不明郵件
5. 頻繁的出現彈跳視窗
6. 工具列突然出現新圖標
7. 出現隨機圖標
8. 密碼無法使用/無法登入
9. 個資和帳號資訊在暗網流通
10. 防毒軟體的警告

電腦遭入侵「跡象」&「應對」

1.您收到勒索軟體訊息:

- 最顯而易見的是，當您開機時不是出現一般的啟動畫面，而是看到勒索訊息，那麼您很有可能已成為勒索軟體的受害者了，它通常會給一個很短的支付時限及說明如何支付贖金，但不幸的是，即便您確實遵守了指示，也有三分之一的機會無法重新獲得這些加密文件的存取權限。

2.電腦跑很慢:

- 當惡意軟體（包括特洛伊木馬、蠕蟲和加密貨幣挖礦）植入於電腦設備時，它們通常會使運行變慢，尤其是加密劫持攻擊，它會佔用大量的效能，當然電腦跑很慢不全然是惡意因素所造成，也有可能是電腦設定不佳等問題。

電腦遭入侵「跡象」&「應對」

3.視訊鏡頭自行開啟:

- 駭客使用的一些間諜軟體除了可以取得您在電腦設備的資料外，還能偷偷打開視訊鏡頭和麥克風，藉由這樣記錄和竊取您和您家人的視頻，進而用於勒索，所以請密切留意視訊鏡頭，檢查它是否會自行開啟，建議最好利用貼布貼住，來確保不會使用到它。

4.您的朋友收到來自您電子信箱不明郵件:

- 還有一個證明您的電腦設備已被入侵的指標是，如果您的朋友和客戶開始收到來自您的不明電子郵件或社交媒體帳戶的垃圾郵件；典型的網路釣魚就是劫持受害者的帳戶，然後向他們的所有朋友發送垃圾郵件或網路釣魚。若所有帳戶都有使用雙重身份驗證(MFA)的機制，則可以輕鬆緩解這種威脅。

電腦遭入侵「跡象」&「應對」

5.頻繁的出現彈跳視窗:

- 廣告軟體通常透過受害者接觸過多的廣告量來讓攻擊者賺錢，因此，如果您的電腦頻繁地彈出式廣告，這代表某處可能安裝了一些惡意代碼或可能不需要的軟體。

6.工具列突然出現新圖標:

- 惡意軟體還可能在您的瀏覽器上安裝其他工具列，如果您發現任何您不認識或不記得下載的內容，則可能意味著您的電腦設備已被駭客入侵；如果您遇到 APT 團體的惡意軟體攻擊，則可能需要將您的電腦設備恢復至出廠設定才能將其刪除，若是PUA (Potentially Unwanted Application，潛在有害應用程式)的話，只要刪除應用程式和工具列就可以了。

電腦遭入侵「跡象」&「應對」

7.出現隨機圖標:

- 當惡意軟體安裝在受感染的電腦設備時，通常會出現新的桌面圖標，只要桌面整齊地排列成少量的文件、文件夾和程式，就可以輕易發現。建議整理一下電腦桌面，以便更好地追踪電腦設備上的圖標

8.密碼無法使用/無法登入:

- 如果駭客入侵了您的電腦設備，他們很有可能已經劫持了各種在線帳戶，例如您的電子郵件，並更改了密碼，將您拒之門外，這也是所有網路攻擊中最嚴重的情況之一。

電腦遭入侵「跡象」&「應對」

9.個資和帳號資訊在暗網流通:

- 如果您收到與您有業務往來公司之資料外洩通知，請務必嚴肅看待並在可以提供第三方確認任何違規行為，可至如HaveIBeenPwned之類的網站進行驗證。另外利用暗網監控工具還可以在網路犯罪的相關論壇搜索您的資料，以更主動的方式來了解您的個資和登錄資訊之暗網流通狀況。還有若您能迅速進行更改密碼、凍結信用卡等行為，也可以降低被駭客利用或攻擊的風險。

10.防毒軟體的警告:

- 來自反惡意軟體工具的警告也應慎重看待，儘管耳聞有假冒的電腦防毒軟體彈跳視窗，但仍請確認訊息是否來自於您購買的電腦防毒軟體供應商，並按照說明嘗試查找並刪除您電腦設備上的惡意文件。

結論

結論

防疫 V.S. 防駭

防疫措施		防駭措施
配戴口罩並定期更換		安裝防毒軟體並更新病毒碼
在外不碰觸眼口鼻		勿點擊不明來源的網址及安裝程式
以正確洗手方式勤洗手	V.S.	定期依照密碼複雜度規則更新密碼
公共場所保持社交距離		企業及機關應落實內外網區隔及防護
機場、港口入出境管制		資安人員應阻絕釣魚網站並禁止電腦連結
感染者應接受隔離治療		受駭電腦應阻斷網路避免病毒橫向擴散

資安實務是一種取捨分析((Trade-off Analysis，TOA)，資安做的越嚴謹大家越不方便且可能影響工作流程；反之越鬆散則越不安全、危險但大家都很方便開心。因此，合理的資安政策要適時的、因地制宜的做取捨分析，或是安排配套措施，取其兼顧營運和風險的平衡點。

結論

Google Cloud台灣技術副總林書平
對於未來防範駭客入侵提出三大努力方向：

1. 強化資安治理、因應新型態威脅
   從策略面、管理面、技術面持續優化資安控管機制，確保資源的有效投入

2. 採取「零信任」存取控管
   應以「身分（identity）」來取代網路作為存取控制安全邊界，且不分內外網來強制實施包括使用者帳戶、權限等在內的存取政策，在「零信任」的安全模式之下，有三大重要的安全原則，包括：[在內外網都要有很嚴格的限制]、[強化帳戶安全並實施裝置政策]、[傳輸加密並強制實施權限檢查]。

3. 建立軟體供應鏈安全
   建立安全開發、安全布署、安全運行的環境，而且還要透過自動化流程減少人為操作，並且盡可能在開發初期發現弱點時就快速修復。

BCCS 漢昕科技

Q & A

BCCS 漢昕科技

感謝各位參與！！