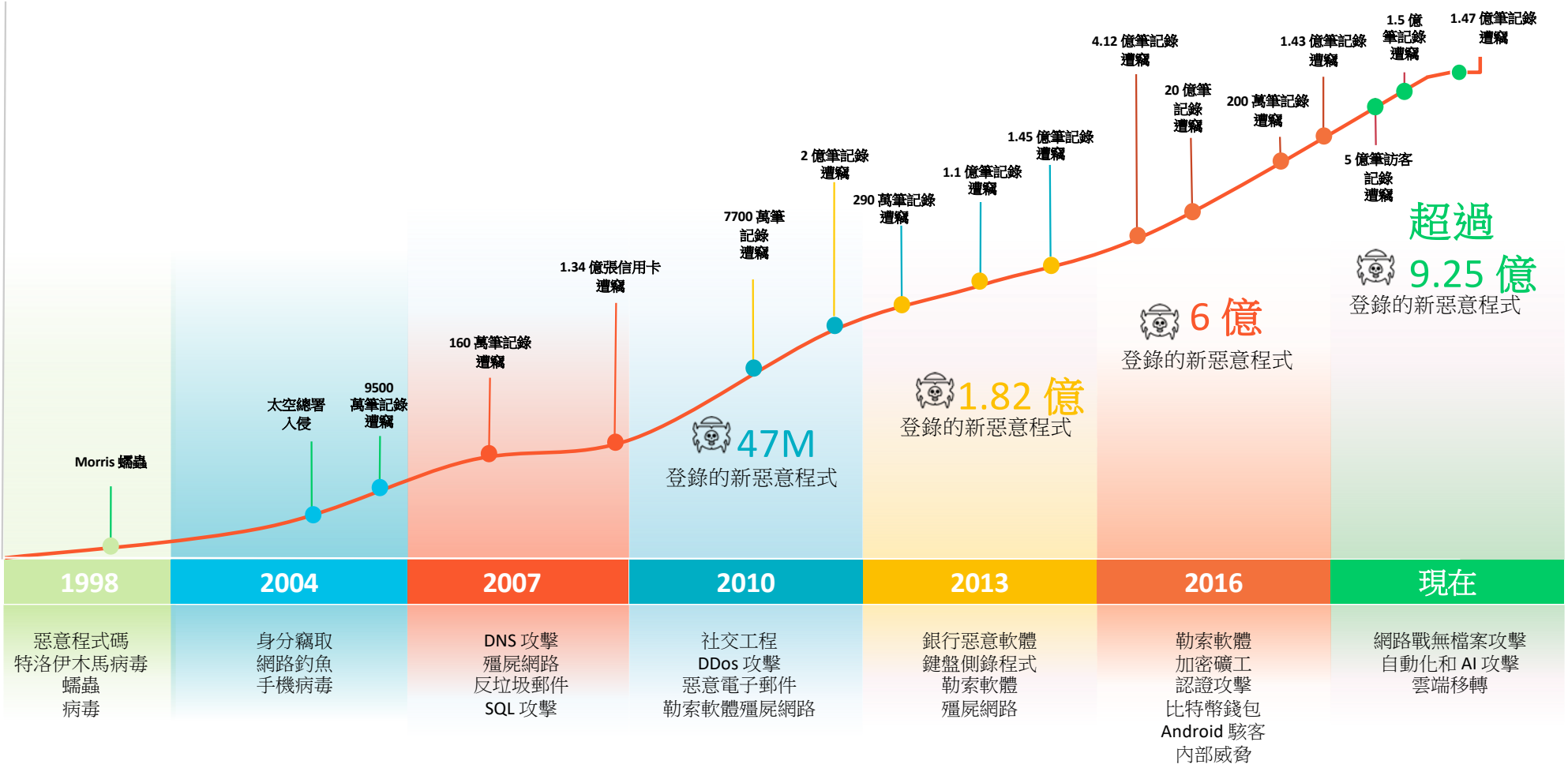
資安威脅、攻擊與防禦

Date: August 7, 2020

資安威脅與攻擊趨勢


Morris 蠕蟲
太空總署入侵
9500 萬筆記錄遭竊
160 萬筆記錄遭竊
1.34 億張信用卡遭竊
7700 萬筆記錄遭竊
2 億筆記錄遭竊
290 萬筆記錄遭竊
1.1 億筆記錄遭竊
1.45 億筆記錄遭竊
4.12 億筆記錄遭竊
20 億筆記錄遭竊
200 萬筆記錄遭竊
1.43 億筆記錄遭竊
5 億筆訪客記錄遭竊
1.5 億筆記錄遭竊
1.47 億筆記錄遭竊
47M
登錄的新惡意程式
1.82 億
登錄的新惡意程式
6 億
登錄的新惡意程式
超過 9.25 億
登錄的新惡意程式
1998
2004
2007
2010
2013
2016
現在
惡意程式碼
特洛伊木馬病毒
蠕蟲
病毒
身分竊取
網路釣魚
手機病毒
DNS 攻擊
殭屍網路
反垃圾郵件
SQL 攻擊
社交工程
DDos 攻擊
惡意電子郵件
勒索軟體殭屍網路
銀行惡意軟體
鍵盤側錄程式
勒索軟體
殭屍網路
勒索軟體
加密礦工
認證攻擊
比特幣錢包
Android 駭客
內部威脅
網路戰無檔案攻擊
自動化和 AI 攻擊
雲端移轉

攻擊鏈

收集情報

計畫攻擊

利用漏洞

隱形感染

執行惡意軟體

已執行惡意檔

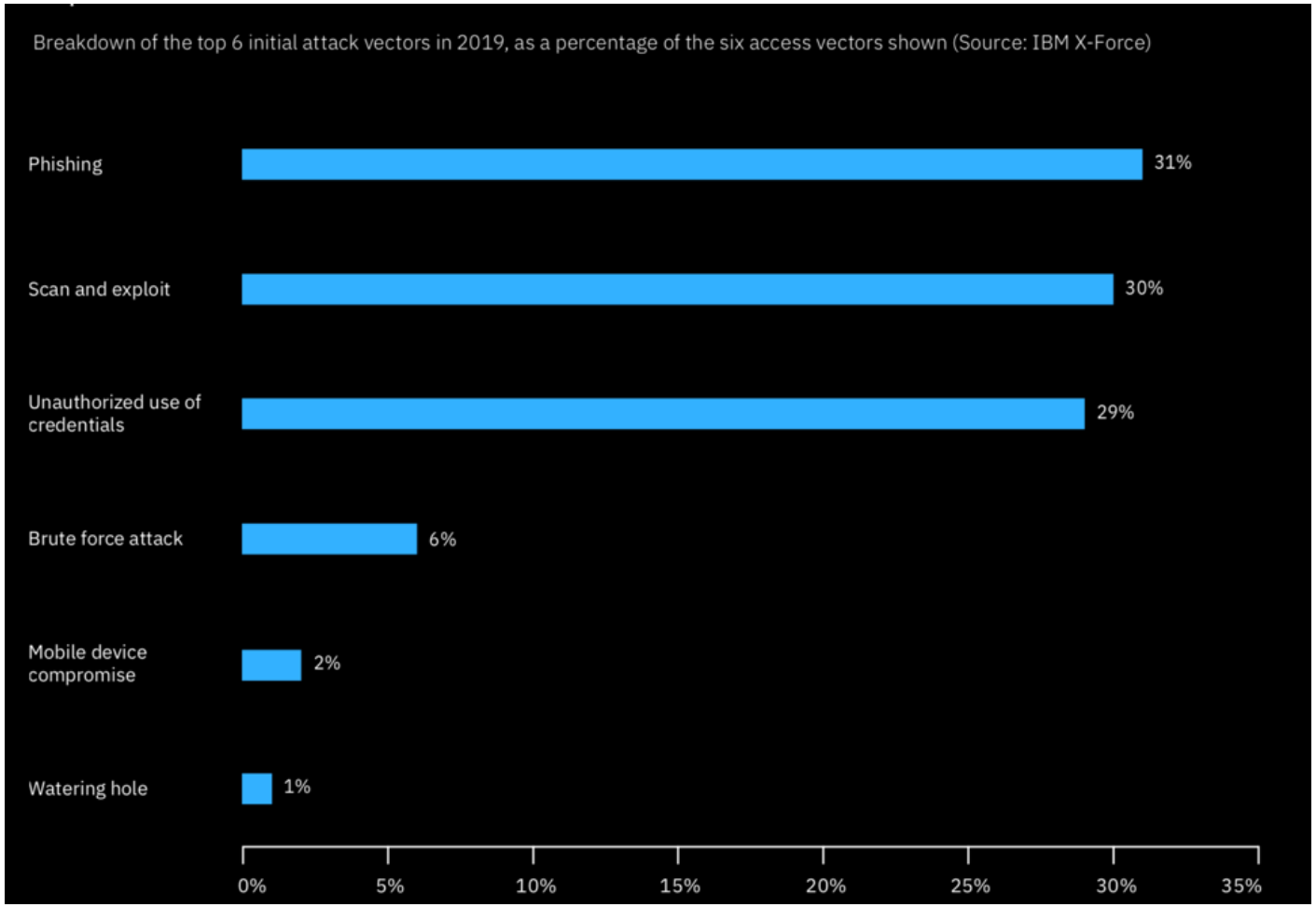
控制通道

惡意軟體
與攻擊者通信

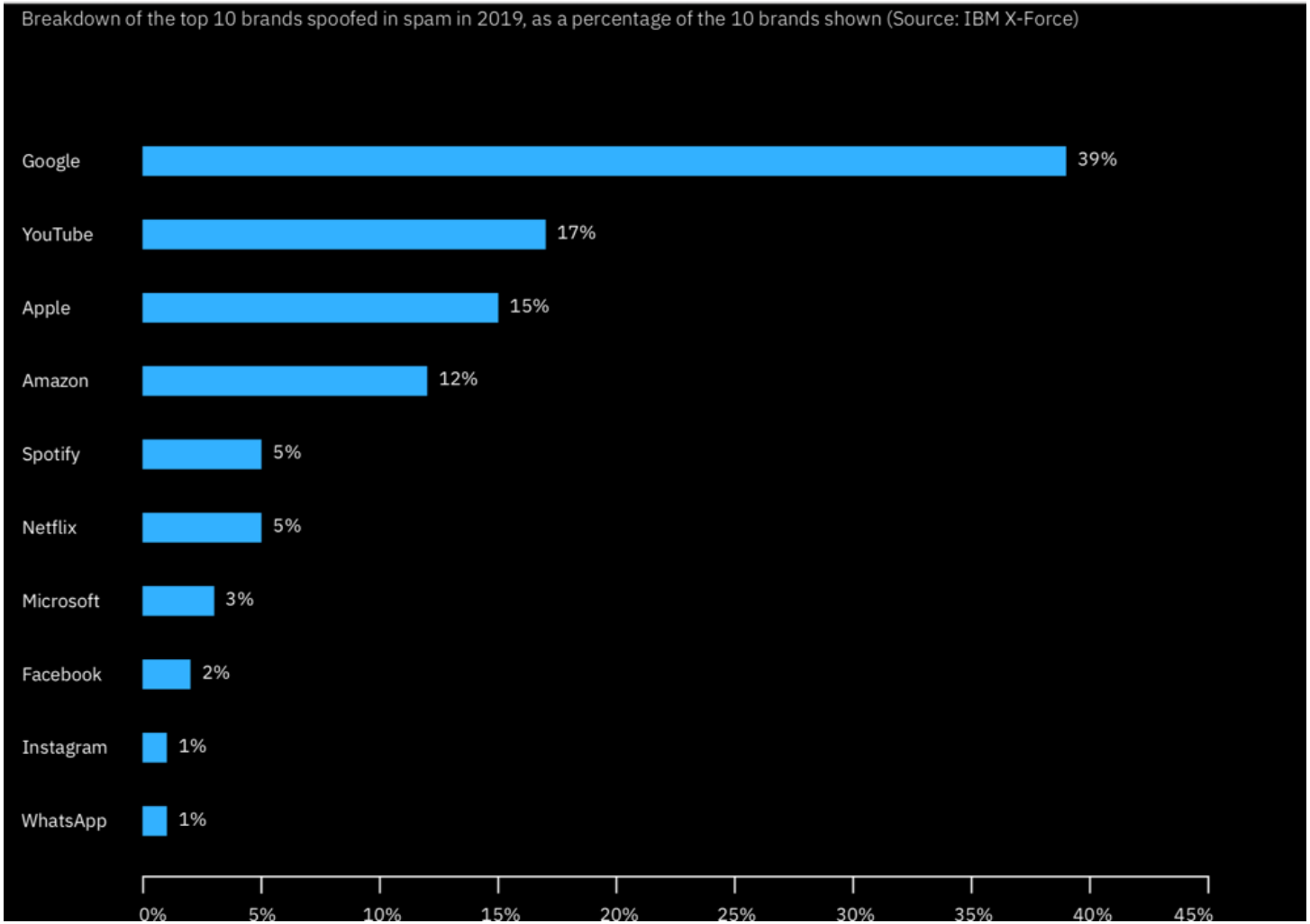
收集贖金、
竊取數據

數據竊取、
妨礙、破壞

2019 Top initial access vectors



2019 Top 10 Brands Spoofed in SPAM



分組討論

Phishing

- 網路釣魚（Phishing，與英語fishing發音一樣；又名網釣法或網路網釣，以下簡稱網釣）是一種企圖從電子通訊中，透過偽裝成信譽卓著的法人媒體以獲得如用戶名稱、密碼和信用卡明細等個人敏感資訊的犯罪詐騙過程。這些通信都聲稱（自己）來自於風行的社群網站（YouTube、Facebook、MySpace）、拍賣網站（eBay）、網路銀行、電子支付網站（PayPal）、或網路管理者（雅虎、網際網路服務提供者、公司機關），以此來誘騙受害人的輕信。網釣通常是透過e-mail或者即時通訊進行。它常常導引用戶到URL與介面外觀與真正網站幾無二致的假冒網站輸入個人資料。就算使用強式加密的SSL伺服器認證，要偵測網站是否仿冒實際上仍很困難。網釣是一種利用社會工程技術來愚弄用戶的實例。它憑恃的是現行網路安全技術的低親和度。種種對抗日漸增多網釣案例的嘗試涵蓋立法層面、用戶培訓層面、宣傳層面、與技術保全措施層面。 From Wikipedia.

設計一個最容易成功的Phishing範例

- 對象：單位內的使用者
- Phishing
  - 媒介：email, SMS, LINE, WeChat, etc.
  - 目標：帳號密碼, 信用卡資訊, 個人資訊, 等等…
  - 主題：
  - 寄件者：
  - 內文 (URL)：


Show Time!

設計一個最有效的組合方法阻止Phishing成功

- 對象：最容易成功的Phishing範例

- 宣導方式
- 獎勵方式
- 懲罰方式
- 技術解決
- 其他方式


Show Time!

案例分析

中油遭受惡意程式攻擊導致資訊系統異常

iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會

文/ 周峻佑 | 2020-07-04 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 1 分享

首頁 > 新聞與公告 > 本部新聞

本部新聞

2020-05-04 15:01 台灣中油公司

台灣中油加油站因遭受惡意程式攻擊資訊系統異常 加油站暫時僅使用現金及信用卡交易

點閱數：686

台灣中油公司因遭受惡意程式攻擊，感染勒索病毒，目前加油站加油部分受影響者為無法使用捷利卡、中油PAY等相關作業，請消費者加油先使用現金及信用卡，其餘生產和供應並未受到影響。

台灣中油指出，資訊系統今天出現操作異常，目前資訊單位已緊急處理中，儘速排除障礙；消費者大部分使用的現金及信用卡交易不受影響，唯牽涉台灣中油內部系統的相關作業如捷利卡、中油PAY等暫停使用，請消費者改用現金或信用卡支付。

武漢肺炎的疫情雖然已經稍微趨緩，但是國家之間的角力並未隨之停歇。與疫情發源地中國相鄰的臺灣，適逢總統就職於5月20日舉行，月初先是兩大石油公司中油與台塑，接連遭受攻擊，接著高科技產業也透過證交所的股市公開資訊站，表示他們遭到勒索軟體入侵。而這一連串發生的事件引起國內高度關注，政府也介入調查，並揭露發現的事證，認為是中國的國家級駭客組織APT 41（Winnti）所為，而且還有10家企業也被鎖定，成為該組織計畫要發動下一波攻勢的目標。

法務部調查局：國內重要企業遭勒索軟體攻擊事件調查

圖片來源: 法務部調查局

法務部調查局分析

- 駭客在數個月之前，就藉由員工的工作站電腦、網頁伺服器，以及資料庫伺服器等管道，入侵公司的內部網路，開始潛伏並加以刺探環境，伺機竊取特權帳號再入侵網域控制伺服器，掌握網域控制伺服器後，駭客利用凌晨時段竄改群組原則（GPO），進行派送駭客執行勒索軟體的惡意排程，一旦員工啟動電腦，就會立即套用上述原則並自動執行，啟動駭客預埋在內部伺服器的勒索軟體，下載到記憶體內執行，加密電腦檔案

- 在加密檔案向企業進行勒索之餘，駭客也在攻擊工具裡埋藏了後門程式，連往位於國外的C&C中繼站，這些中繼站的主機，駭客是向美國境內雲端主機（VPS）服務供應商租用，並使用滲透工具Cobalt Strike遠端存取控制

建議採行多重防護措施

- 「零信任」（zero trust）設計網路安全
- 端點偵測及回應（Endpoint Detection and Response: EDR）保護個人電腦與伺服器
- 特權帳號管理（ Privileged Access Management: PAM ）確保有權限的帳號被適當管理
- 多因子驗證（Multi-Factor Authentication: MFA）單一密碼驗證登入已經是過去式，多因子驗證才能確保帳號安全
- 安全資訊事件管理系統（ Security information and event management: SIEM ）需要SIEM彙整、分析、管理資安事件，避免被大量的雜訊淹沒
- 防火牆(NGFW)仍是網路流量管制的必需品，要能識別應用程式、並阻擋C&C回報
- 資料備份(Data Backup)仍是最後的資料保護防線

「零信任」（zero trust）

https://www.ithome.com.tw/article/124684

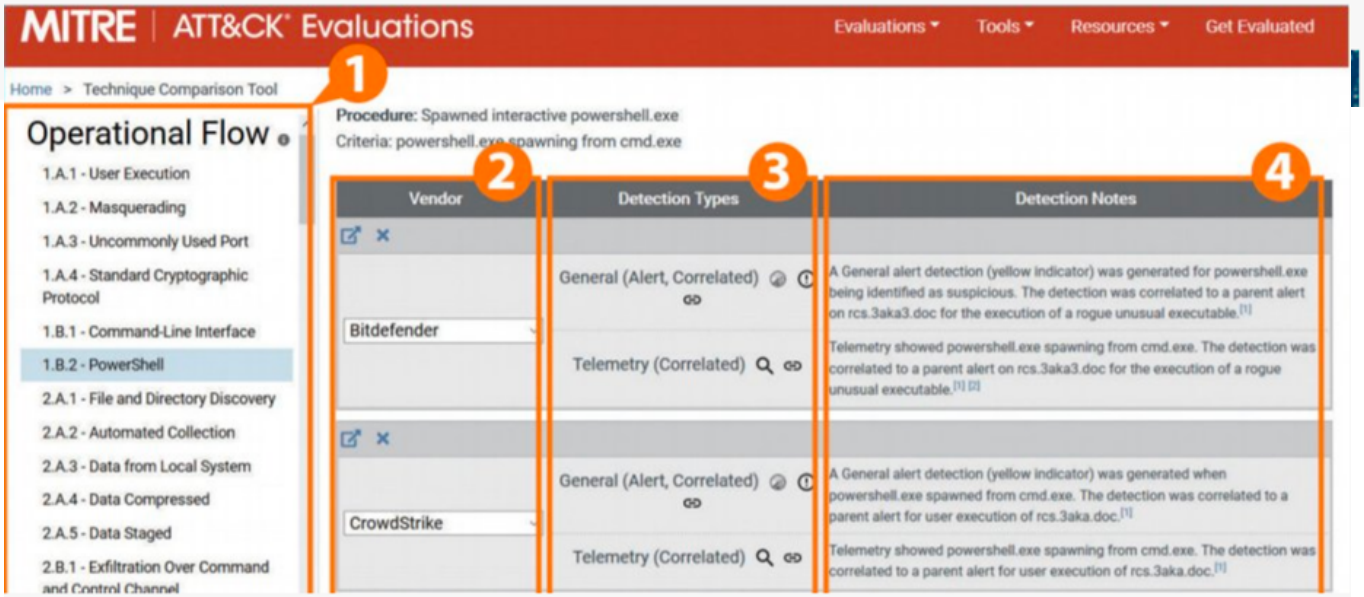
端點偵測及回應（EDR）

技術文章

端點防護是勒索軟體最終抵禦的戰場

不光只是阻絕威脅，同時對於潛在的勒索軟體攻擊事件調查，端點電腦更是採集證據的重要來源

文/ 周峻佑 | 2017-12-30 發表



https://www.ithome.com.tw/tech/119815
https://ithome.com.tw/news/137821

特權帳號管理（ PAM ）

- 特權帳號的存取是通往最重要資訊資產的途徑
- 犯錯乃人之常情
- 要使用特權帳號存取的不止人類
- 特權帳號存取存在於所有員工工作站和終端上
- 稽核和合規圍繞特權帳號存取進行

https://www.digitimes.com.tw/iot/article.asp?cat=130&cat1=40&id=0000581465_OE63GL9675S4GW4104509

多因子驗證（MFA）

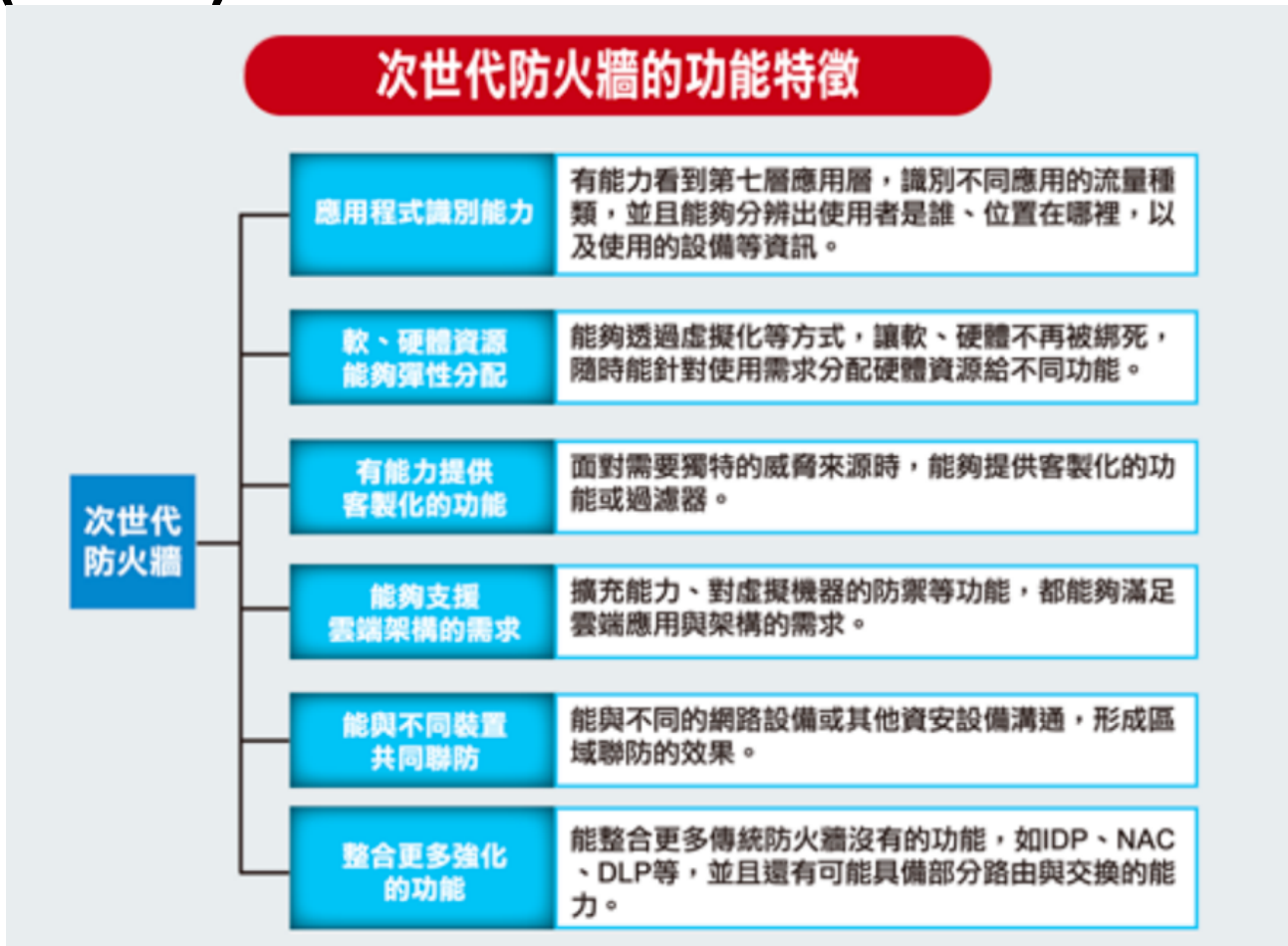
- Something you have：具有權限者擁有的特定實體物品，如具備有密鑰的USB、通行證、鑰匙等
- Something you know：具有權限者所知道的，如密碼、特殊的手勢軌跡、啟動的按鍵順序等
- Something you are：具有權限者所具備的，如指紋、眼睛虹膜、聲紋等

安全資訊事件管理系統(SIEM)

- SIEM包含：前端的事件收集器(connector)、中間的日誌管理系統(logger management)和後端的事件關連分析平台(correlation)
- 網路罪犯在被發現之前，平均已經在網路內部 191 天。SIEM可幫助去除雜訊來保存隱密的威脅入侵資訊，主動式減少偵測時間並可能在攻擊者傷害發生之前阻止它發生
- 每天自動對數百萬到數十億的事件進行排序，以偵測異常和惡意活動、識別及分組相關事件，並只對最嚴重的威脅產生已設定優先順序的警示

https://www.netadmin.com.tw/netadmin/zh-tw/trend/FFD3E89AED9E4345A0FE6355906A3E94

防火牆 (NGFW) – 管控應用程式的「次世代防火牆」



https://www.ithome.com.tw/news/95997

資料備份(Data Backup)

- 即使付了贖金也有19%拿不回資料，最理想的辦法就是平常就得好好備份資料

https://www.ithome.com.tw/voice/118514
https://www.ithome.com.tw/news/118046

Thank you