bsi. ...making excellence a habit.™

2019 年網路安全趨勢

BSI CSIR 網路安全和資訊韌性白皮書

摘要

BSI 網路安全和資訊韌性（Cybersecurity and Information Resilience, CSIR）分析了 2019 年網路環境的新興趨勢，包括這個充滿變化和挑戰的領域中，未來的威脅和機會將如何演變。

本白皮書重點介紹了網路威脅、目標產業、網路相關法規、科技演進和具體解決方案的下一步發展。

在網路威脅中，我們分析了針對 Linux 和 MacOS 的惡意軟體、UEFI 惡意軟體和 Crypto Mining 挖礦惡意軟體的氾濫情況。然後，我們把重點轉向未來最常見的目標產業、即將發行的「電子隱私權」法規和相關的國際標準。

本文最後提出了與科技發展的相關風險和未來解決方案。當然，未來不可能完全準確預測，然而，科技變化快速雖能促進創新，但更強的威脅隨之而來，每個組織都必須規劃並準備好自己的防禦工事。

Cyber threats

網路威脅

Linux 和 MacOS 作業系統惡意軟體

幾年前，人們認為 Linux 和 MacOS 作業系統（OS）比較安全，這種理解或許沒錯，但隨著科技發展，惡意攻擊的目標也隨之演進。

我們可以看到鎖定 MacOS 裝置的惡意軟體不斷增加，在過去兩年中，鎖定 Linux 的惡意軟體卻有更明顯的增長。例如，防毒軟體測試公司 AV-TEST 就強調：從 2016 年以來，Linux 惡意軟體的開發數量增加了三倍。這一事實令人擔憂，其原因很多， 簡述如下。

首先，如果大家一直認為以 Linux 為基礎的系統比較安全，那麼，我們就會減少資安控管，甚至不進行資安控管。其次，大多數 IoT（物聯網）裝置和許多基於 Web 的系統都使用 Linux 作業系統，如果這種趨勢持續上升，即可能增加這些系統的資安漏洞。

2019 年的解決方案是重新分析風險，並在基於 Linux 的系統上執行安全評估測試。此建議符合 PCI DSS（支付卡行業資料安全標準）3.2.1 版要求；該標準指出：對於被認為通常不受惡意軟體影響的系統，應執行定期評估，辨識與評估不斷變化的惡意軟體威脅，以便確認此類系統能否繼續不安裝防毒軟體。

UEFI 韌體惡意軟體

惡意軟體通常利用作業系統（OS）登錄用戶的管理者權限。

因此，處理此類感染的最安全作法就是重新安裝作業系統。遺憾的是，您無法如此處理 UEFI（統一可延伸韌體介面）惡意軟體的感染，因為針對 UEFI 設計的惡意軟體可以利用 UEFI（新一代的 BIOS）韌體組件中的漏洞，來完全控制系統，並且可以在重新安裝作業系統後繼續使用。例如，電腦安全軟體提供商 ESET 在 2018 年發現了命名為「Lojax」的 UEFI 惡意軟體；此惡意軟體主要使用於網路間諜活動，是利用了「LoJack」(一種防盜追蹤軟體）中的漏洞。

在 2019 年，由於 UEFI 惡意軟體的頑強和效率對駭客具有吸引力，預期它還可能繼續增加。為了緩解這些威脅，最重要的是不斷更新作業系統的韌體，且於必要時，採用實體設備與使用者行為分析（Entity and User Behaviour Analytics, EUBA）解決方案，透過行為分析來偵測危害模式。

Crypto Miner 挖礦惡意軟體

在 2018 年，安全意識提升和資料解密工具的開發，減少了勒索軟體的攻擊，但也迫使駭客開發出替代方案來求取金錢利益。

隨著虛擬加密貨幣蓬勃發展，Crypto Miners 惡意軟體成為獲取收益的完美替代方案。Crypto Miners 惡意軟體濫用受感染裝置的計算能力來求解數位貨幣交易的加密計算。以此過程來獲得獎勵貨幣，其利潤非常高，但被追溯的風險卻很低。

我們在 2018 年雖然見證了 Crypto Miners 惡意軟體的崛起，但從趨勢來看在 2019 年很可能會發生焦點移轉，也就是以瀏覽器為基礎的 Crypto Miners 惡意軟體減少，但基於作業系統的 Crypto Miners 惡意軟體增加。可能見到的是，精密複雜的網路釣魚活動和利用未修補漏洞的情況將越來越多。

Targeted sectors

目標產業

關鍵基礎設施

網路防禦的投資漸增，及一些國家的攻擊性網路安全策略（例如，俄羅斯涉嫌干涉美國總統大選、朝鮮駭客團隊 Lazarus Group 涉嫌發動 WannaCry 攻擊），讓我們認為，地緣式的網路情境將發生變化。

在 2019 年，關鍵基礎設施將繼續牽涉地緣政治的網路戰佈局，但可能會遭受破壞性和侵略性的網路攻擊。保護關鍵基礎設施的唯一方法是保護其網路、內部邊界和供應鏈。

為了引領各國，歐盟發布了「網路與資訊系統安全指令」（NIS 指令），要求成員國在 2018 年 5 月 9 日之前，將 NIS 要求轉換為各國法規。也就是說，2019 年關鍵基礎設施保護的趨勢包含各成員國的立法工作，當然還包括所有相關的 GRC（治理、風險管理和合規）及技術投資。

汽車

隨著無人駕駛和輔助駕駛汽車等新興科技的發展，汽車行業將面臨越來越多的安全挑戰。

自動機器的想法並不新穎，但 100% 無人駕駛車的概念已開始出現於我們的日常生活當中：許多汽車公司已經朝這個方向發展。

這項令人驚豔的創新帶來諸多好處，但隨之而來，有心人士也可能會瞄準自動駕駛汽車。最常見的風險將是鑰匙遭駭客篡改、個人資料外洩、勒索軟體，以及「車輛到車輛」（Vehicle-to-Vehicle，V2V）和「車輛到交通基礎設施」（Vehicle-to-Infrastructure，V2I）之間的通信服務遭拒。

這項現代化將牽連許多網路安全課題，例如：需要確保系統的韌性、強大的加密功能、完整性、和高度可用性。測試這些系統的機密性、完整性、可用性和韌性，將是製造商在 2019 年需要面對的關鍵趨勢。

Regulations

法規

ePrivacy Regulation 電子隱私條例和相關國際標準

目前 GDPR（一般資料保護規範）已經全面實施中，而歐盟正準備發布新的法規。

《電子隱私條例》（Regulation on Privacy and Electronic Communications, ePrivacy Regulation）的提案已獲得批准和修訂，最終版本預計將於 2019 年公佈。這將進一步強化電子通信的機密性。擬議中的法規具有與 GDPR 相同的制裁力（罰鍰佔全球年營業額的 4%或高達 2000 萬歐元），但有更多技術要求。

這表示隱私和資料保護即將邁入一個新的時代，而且重心將從政策制定者和法律顧問轉移到工程師身上，他們必須處理架構複雜的遵循性要求和各種整合。

認知到此趨勢，ISO（國際標準化組織）也將釋出新標準，並可能在 2019 年發布：

- ISO/IEC 29101「資訊安全技術隱私框架標準」，用以釐清在資訊科技運用上處理個人可識別資訊（PII）的管控疑慮。
- ISO/IEC 19086-4 雲服務水準協議（SLA）框架：安全和 PII 保護，為處理 PII 的雲端服務設置 SLA。

相關權責人員在考量電子隱私條例時將會面臨新的任務，因為歐盟的合規方案建議採用普遍公認的標準做為指引。

Technology

科技

醫療器材和生物奈米物聯網（IoBNT）

越來越多的醫學研究涉及基因組編輯和連網醫療裝置，這將為我們的生活帶來益處—以及風險。

根據 ENISA（歐盟網路與資訊安全局）的白皮書，科學家正在研究是否可能結合網際網路裝置與微型化和生物程序，從而產生所謂的 IoBNT。這些發展將伴隨著前所未有的資安挑戰，例如：需要增強資安控管的穩健性、高度的韌性和新的跨學科方法，來結合資安工程師、醫生、研究人員、法律和道德顧問的工作成果。

到 2019 年底，我們可能會開始看到對於這些複雜科技的資安和道德意涵的相關討論。

Solutions

解決方案

進階惡意軟體偵測 Advanced malware detection

在面對無檔案惡意軟體或 APT（進階持續性威脅）時，傳統的、以比對特徵為基礎的**端點保護解決方案表現得很沒有效率，因為根本無從偵測到它們。**

因此，惡意軟體的擴散和設計都朝著這個方向發展，造成還在仰賴這些傳統技術的系統變得更加不安全。

為了避免這些威脅，資安供應商開發了進階惡意軟體偵測的概念，透過持續分析網路端點的活動，以便發覺有規律的行為（例如，透過機器學習演算法）並偵測可疑行為。此科技被稱為實體設備與使用者行為分析（EUBA）。

在發現 68%的威脅來自外部（Verizon 2018 資料洩漏調查報告）之後，我們必須重新評估傳統以特徵為基礎的防毒軟體，以確保充分涵蓋惡意軟體風險。在 2018 年，我們已經觀察到進階惡意軟體偵測應用的增長，但在 2019 年，這些科技將展示其真正潛力。這是因為機器學習演算法只有在獲得大量行為模式之後才可最有效運作。

藉由不斷提高 Office 365 對用戶端點、電子郵件和網路惡意活動的能見度，微軟在這個領域可能變得越來越強大。再透過其「單一管理介面」（single pane of glass）途徑和資安管理遊戲化，微軟更可能成為資安市場中最大的參與者之一。

主動防禦網路釣魚 Active anti-phishing

大多數網路攻擊的載體（主要是惡意軟體）都透過針對公司和私人電子郵件的網路釣魚活動來傳遞。

員工訓練和意識提升可以幫助避免一些容易鑑別的網路釣魚攻擊，但為了實現最高等級的保護並反擊進階網路釣魚活動，組織應實施主動防禦網路釣魚解決方案。

這些解決方案基於組織政策和程序修訂、使用者培訓和意識，還有以人工智慧（AI）為基礎的科技。AI 反網路釣魚解決方案將分析收到的電子郵件以偵測可疑模式。這些解決方案可用來強制執行重新設計的政策和程序、執行模擬攻擊和干預可疑的行為。真正有效的解決方案將組合郵件過濾器（SPF、DMARK、DKIM 檢查）、垃圾郵件防禦系統、網頁過濾器、沙盒技術和下一代 EUBA 等。

裝置和服務的驗證方案

要減輕未來風險，在開發的早期階段就考量資安控管，永遠是一項簡單卻有效的解決方案。

但是，如果沒有明確且成熟的流程，這種方法可能引發不受控制的後果，因此，裝置和服務的驗證因運而生。我們認為以公認的資安標準為基礎的驗證方案日益增加，將是網路安全解決方案的未來趨勢。

例如， 2018 年，美國 FDA（食品藥物管理局）一對醫療器材市場一發佈了「醫療器材網路資安管理上市前提交內容」（Content of Premarket Submissions for Management of Cybersecurity in Medical Devices）新草案。這份文件可幫助器材製造商為其醫療器材做有效的網路安全規劃，顯示醫療器材一包括所有互聯裝置或服務一的網路安全需求增加已成明顯趨勢。

結論

2019 年惡意軟體攻擊和網路釣魚活動將持續為網路安全環境帶來威脅，並將更具持續性與不易偵測等特點。

我們需要高水準的專業技能、知識和跨多學科領域的方法，來因應不斷增加的法律、法規和標準。創新科技一例如 100%無人駕駛的汽車和互聯微型醫療裝置等一將佔據主導地位，但不幸的是，未知的網路風險也將伴隨而來。

同樣的，在地緣政治的網路戰中，關鍵基礎設施也將被列為主要攻擊目標；對此，組織應預測即將到來的威脅、以新方法修復漏洞和降低風險，優化自身的網路安全態勢。因為這個原因，有必要設計由上而下的網路安全治理策略，並透過政策、程序和更新科技來加以實施。組織要保障資訊安全必須在早期執行階段就考量資安控管、進行威脅模型分析且使用階層式方法，提供資安解決方案。

BSI CSIR一讓您和您的組織實現強化且永續的資訊韌性。

BSI 資訊安全與網路安全系列課程

資訊安全	個資管理	雲端安全	品質管理	營運持續	產業資安
ISO 27001 資訊安全管理系統 **基礎課程** **建置課程** **風險評鑑課程** **內部稽核員課程** **主導稽核員課程**	BS 10012 個人資訊管理系統 基礎課程 建置課程 內部稽核員課程 主導稽核員課程 主導稽核員/稽核員轉版課程	雲端服務資訊安全管理系統 Cloud 主導稽核員課程	ISO 20000 IT 服務管理系統 基礎課程 建置課程 內部稽核員課程主導稽核員課程	ISO 22301 營運持續管理系統 基礎課程 主導稽核員課程	PCI DSS 支付卡產業資料安全標準 以 PCI DSS 強化電子支付服務的資訊安全管理及法規遵循課程 內部稽核員課程 主導稽核員課程
GDPR 歐盟一般資料保護規範 **基礎課程**	ISO 29100 隱私框架基礎課程 主導稽核員課程	ISO 27017 & ISO 27018 建置課程	NIST 網路安全框架 建置課程	BSI 營運衝擊分析課程	ISO 27799 健康醫療資安基礎課程

課程詳情請洽 BSI 訓練學苑：02-26560333 | training.taiwan@bsigroup.com

- **洽詢 BSI |** 稽核驗證、產品測試、BSI 訓練學苑、VerifEye 認證平台、BSOL 標準資料庫

BSI英國標準協會
T: +886 2 2656 0333 | E: infotaiwan@bsigroup.com | www.bsigroup.tw