主動防禦搶先機 端到端全面阻擋新威脅

頭痛醫頭、腳痛醫腳的局部措施及事後修補，難以因應動態變化的資安威脅，尤其在即時協同合作、遠端辦公等需求持續攀升的現況下，唯有讓安全深化成為每項產品的原生 DNA，從開發階段就進行演練及優化，主動防堵潛在的資安漏洞，並確保與時俱進的防禦力。

早在 2004 年，微軟就於全公司實施安全開發生命週期（Security Development Lifecycle；SDL）政策，主要目的是為了確保所有軟體產品的安全性，並將資安全及個人隱私的考量，深入地整合至微軟自身的文化與推出的軟體產品。

為時至今，微軟在資安的承諾與投資有增無減，而且轉守為攻，持續尋求更有效的作法來增進微軟產品的安全性。舉例來說，以主動出擊的作法尋找產品的資安漏洞或弱點，搶先在駭客或惡意人士探測到之前，完成修補方案或強化措施；此外，內建於全線產品及服務的安全相關功能也持續精進，打造主動防禦的守備空間。

橫跨軟體工程生命週期的資安整體對策

以整體全面的觀點，將安全性融入軟體工程的生命週期，正是微軟長期以來採取的對策，實際行動包括：

- 在最初的功能設計階段就納入安全考量。
- 發展相關工具和作法以主動找出程式碼裡的漏洞與弱點。
- 針對 Windows 環境提供解方，大幅提升錯蟲被探測利用的難度。
- 攜手微軟世界級的滲透測試團隊，實測產品的安全界線，在影響用戶之前預先修復。

藉由這些作法，不但持續提升 Windows 平台的安全性，而且能在駭客或惡意人士發動攻擊之前，盡可能地找出並防堵最多的漏洞或弱點，免於淪為資安破口。此外，微軟的滲透測試團隊則熟知不斷進化及演變的威脅場景，對產品安全界線的持續測試，就成為提升安全性的關鍵助力。

值得一提的是，微軟團隊早在數年前就開始聚焦在尋找遠端網路的弱點，並阻止類似 WannaCry 和 NotPetya 勒索病毒事件的爆發。舉例來說，近期發現並修復的重大漏洞就與遠端通訊工具有關，影響所及包括 RDP（Remote Desktop Protocol）伺服器端和用戶端，但主動出擊的策略發揮顯著成效，成功阻擋了新型的 WannaCry 勒索病毒。

自製工具及探測技巧的精進

在主動出擊的過程裡，最大的挑戰之一就是分析數量龐大的程式碼。光是 Windows 就有 570 萬筆原始程式碼檔案，每天由分佈在全球 440 個據點的 3,500 位工程師進行超過 1,100 次的 PR（pull requests），如此快速的步調不僅催生出許多新功能，也有助於深化 Windows 安全性。

微軟團隊採行常見的模糊測試以快速探索及評析大量的程式碼庫，差別在於內部自行研發的模糊測試技術可進行更深入的探測，因而能以更快速度找到新錯蟲，例如：在 SMBv3（Server Message Block Version 3）發現並於 2020 年 3 月 12 日發佈修復程式的遠端程式碼漏洞。

被稱為「TKO」的全系統模擬工具是微軟團隊的自製成品，用於探測及內觀 Windows 元件，提供全系統模擬執行、記憶體快照拍攝及其他創新功能。而在 SMB 網路漏洞探測的過程裡，更帶來許多獨特效益，例如：

- 從任何程序狀態進行快照及探測的能力。
- 高效率回存原始狀態以進行快速迭代。
- 橫跨所有程序完整收集涵蓋範圍程式碼。
- 可大規模探測系統但同時免於過度干擾。

緊密結合相關工具及專家實力，微軟團隊同時橫跨使用者與核心模式進行作業，大幅縮減命中目標前的尋覓過程。以 SMBv3 的狀況及影響層面來看，過往的首要作法多是解析網路傳輸協定，現在則是對 SMB 程式碼庫進行稽核及探測，初步了解其架構與資料流，掌握協定狀態空間的規模，就可齊備展開探測所需的資訊。

Windows 10 長期耕耘的關鍵助力

過去數年間，微軟持續鞏固 Windows 10 安全性的作法，正好也為對抗遠端網路漏洞預先設下防線，包括 ASLR（Address Space Layout Randomization）、CFG（Control Flow Guard）、InitAll 與 HVCI（Hypervisor-enforced code integrity），為企業組織的防禦者爭取了額外的寶貴時間來修補及保護他們的網路，而上述多重作法的加乘效應，也造成攻擊者必須付出更多時間和成本才能取得有效的探測成果。

在微軟攜手 PC 廠商推出的 Secured-core PC 計畫裡，前述的防範措施不僅都是預設功能，而且全面涵蓋虛擬化、作業系統、硬體與韌體的防護。進一步搭配 Microsoft Defender 進階威脅防護，則可提供端到端的完備防護來對抗進階威脅。

除了致力降低資安漏洞被探測及利用的機率，微軟也持續加強化威脅防護機制本身的進化能力，例如：微軟威脅防護（MTP）不僅內建 AI 和自動化功能的整合體驗，利用並整合領先業界的防護、偵測、調查和回應技術，搭配持續彙集的集體知識和功能來累積更佳體驗，協助保護使用者、端點、雲端應用程式和資料。

資安威脅早已不是制式化的一成不變，透過主動出擊的作法來強化防禦者，協助他們從被動反應，轉為運用他們獨特的專業知識來阻止惡意攻擊者，進而發揮制敵機先的效益，資安抓漏正是實現這個目標的關鍵環節。

隨著疫情而來的資安威脅如何防範？

在疫情大流行期間，網路釣魚攻擊正逐漸增加。而且，越來越多的人正在進行遠端工作，並將新裝置連接到商務網路。了解 Microsoft 威脅防護如何利用 AI 自動偵測、回應並讓跨網域的事件相互關聯，協助您迅速保護遠端工作力。
https://aka.ms/AA8g52q