2020網路安全真相、數據與統計

從惡意軟體趨勢到預算的轉移，透過數據來量化產業的狀態。

文／Josh Fruhlinger 譯／Nica

你是否正在尋求明確的數字來支持你對現今資安世界發生的一切的理解？我們深入探索這個產業領域的調查與研究，包含：資安管理者如何應對持續發生的事件。如果你想知道哪些系統最容易被入侵、哪個惡意程式名列前茅，以及多少人花錢解決這些問題，請詳閱本文。

九大網路安全統計速覽

- 94%的惡意軟體透過電子郵件傳送。
- 在被報導的資安事件中，超過 80% 的成因來自釣魚攻擊。
- 釣魚攻擊每分鐘造成 17,700 美元的損失。
- 60% 的外洩事件所利用的漏洞已經有修補程式，但卻沒有套用所致
- 63% 的企業認為他們的資料在近 12 個月內可能因為硬體或晶片的漏洞遭到感染
- 針對物聯網設備的攻擊在 2019 上半年增加了兩倍
- 無檔案攻擊在 2019 上半年成長 256%
- 資料外洩平均耗費企業 392 萬美元
- 有 40% 的 IT 主管認為網路安全的工作最難補足人力。

漏洞之年

讓我們從基本開始：無論在這篇文章或是其他網路安全文章中，你聽到多新穎或是奇特的漏洞，總是會有一個一支獨秀的漏洞！根據 Verizon 針對數千筆資安事件的調查，發現幾乎所有惡意軟體都是透過電子郵件進入電腦（約佔 94% 的事件）。在這些相關新聞中，超過 80% 起因於社交工程，也就是釣魚攻擊，透過說服使用者來安裝惡意軟體。所以如果你想改變你的防禦狀態，這會是一個最初應該被防範的地方。（當你以為釣魚攻擊來自一些險惡的東歐或是奈及利亞時，其實 40% 的釣魚指令與控制伺服器位在美國。）

當然，這並不表示其他弱點不重要。常見漏洞與揭露資料庫（CVE）列出 11,000 個常用的系統或軟體存在可以被攻擊的弱點，截至 2019 年中，有 34% 的弱點仍然沒有修補程式可以使用。微軟的 Equation Editor 弱點 CVE-2017-11882，就是說明弱點修補程式如何發揮作用的好例子，因 IT 部門使用修補程式或自 Windows 7 更新伺服器，讓透過這個漏洞傳遞的惡意軟體在幾個月內驟降超過 70%。僅僅修補程式的存在不能解決一切：Security Boulevard 指出，有 60% 涉及可攻擊弱點的外洩事件，是存在修補程式但卻沒套用。

若想深入了解漏洞的世界，我們需要更了解電腦內部，包含了解 BIOS 等（編譯：要深入了解漏洞的世界可能不是企業最需要優先執行的項目之一）。Dell 在其報告的結論中指出，63% 的公司認為他們的資料有可能在近 12 個月內，由於硬體或晶片的安全漏洞遭到感染。（同份調查中發現只有 28% 的公司滿意其供應商的硬體

資安管理，這結果不足為奇）

最後一個可能的攻擊表面（attack surface）可能是：現今從生產製造、到家中的播放音樂設備 - 無所不在的物聯網設備。Mirai 殭屍網路事件發生之際，資安專家便對物聯網提出警告，只是情況惡化的更快：根據 F-Secure 估計，針對物聯網裝置的攻擊在 2019 年上半年增加了兩倍。

讓人訝異的是，佔盡新聞版面的勒索軟體，竟排在本項研究的倒數第一，每次攻擊平均「僅」造成企業損失 646,000 美元。

惡意軟體走向

惡意軟體不斷嘗試利用這些弱點。根據 Kaspersky 表示，依據他們的網路防毒平台，在 2019 年就識別出 24,610,126 筆「新的惡意物件」（uniqle malicious objects），比 2018 年多了 14%。整體說來，根據其說法將近 20% 的網路使用者成為某些類型惡意攻擊的目標，但這些目標並不會全部被攻擊，因為攻擊者會針對比較有利益的目標進行攻擊。舉例來說，Malware Bytes 報告指出，惡意軟體攻擊一般消費者事件已經減少 2%，但針對商業組織的威脅則增加至 13%，後者很顯然的成為駭客們的目標。

過去這幾年，哪些特定類型的惡意攻擊成為注目的焦點？Malware Bytes 指出，被稱為駭客工具的一類惡意軟體的感染率增加了 224%（駭客工具基本上具有探測系統和網路漏洞的功能，並且可以透過下載惡意程式碼來利用這些弱點）。

另外，有一些其他型態的惡意軟體在 2019 年也非常盛行。無檔案惡意程式 - 攻擊碼只存在記憶體中且不會在磁碟寫入檔案，正持續發酵。Trend Micro 表示，無檔案攻擊在 2019 年上半年成長了 256%。而另一個即將爆發的威脅則是網頁測錄（web skimmer），犯罪集團將程式注入到伺服器端、有時甚至安裝於用戶端中，以便側錄信用卡資料，這種攻擊驟增了 187%。

困擾全球超過五年的銀行木馬程式 Emotet，這段時間持續精進並在 2019 年捲土重來，如今它主要用來散佈其他木馬，如著名的 TrickBot。據 Cofense 指出，2019 年的最後三個月，Emotet 利用了超過 290,000 封感染的電子郵件散佈惡意軟體，其中內含 33,000 種獨特的附件檔案。

資安失誤的代價

據聞銀行搶匪 Wilie Sutton 曾說過，搶銀行是因為「錢就在那」。Verizon 的資料外洩報告也證實網路犯罪背後的主要動機：有 71% 外洩事件為財務動機。不過顯然網路犯罪的收獲，是守法公民的損失。

還記得前文提到，電子郵件與釣魚攻擊仍然是惡意軟體的主要傳遞方式？其實，它造成的傷害相當驚人。RiskIQ 粗估，因釣魚攻擊而造成的損失為每分鐘 17,000 美元。但這還只是損失的開始。如果攻擊事件涉及資料外洩，對受害者而言，並非所有事情都像 Equifax 被駭事件一樣付出昂貴的代價，但它們仍然很糟糕：IBM 對超過 500 間公司企業所作的外洩事件調查中，受影響企業的平均財務損失（包括罰款和工時損失）約為 392 萬美元。

Accenture 對各種類型的網路攻擊的成本進行了研究，得出了有趣的結果。惡意軟體榮登最昂貴榜首：這個攻擊造成受害者 260 萬美元的損失。或許更讓人訝異的是，佔盡新聞版面的勒索軟體，竟排在本項研究的倒數第一，每次攻擊平均「僅」造成企業損失 646,000 美元。而且這包括諸如生產力降低之類的附加成本，而不只是勒贖贖金本身：此類攻擊中的贖金支付通常令人驚訝地低。

Data Breach Today 將 2019 年第三季平均支出定於 41,000 美

元。請注意，由於企業組織擁有妥善的備份政策，或者決心不屈服的組織有時候會拒絕支付贖金，因此支出可能為零。實際上，支付贖金的受害者所佔百分比因國家而異：加拿大有 77% 的受害組織願意支付贖金，而美國人只有 3%。德國和英國介於這兩個極端之間。

2019 年最大的支出案例之一是，公司正在決定希望獲得外部網路安全服務的幫助。

最後，切記：就算你完全沒被駭，不當的安全控管也會讓你付出代價，因為法規單位正逐步讓不安全的或危害使用者的資料作業方式在財務上付出代價。例如，去年 Google 因不遵守 GDPR 的規定而不得不在法國支付 5700 萬美元的罰款。

預算及花費優先權

隨著這些潛在損失的迫在眉睫，企業意識到他們必須花錢保護自己，並以此規劃預算。〈2020 State of the CIO〉研究報告的受訪者確實感到擔憂：34% 的人將安全和風險管理視為其組織整體 IT 支出的第一大推動力。

IDG 的 Security Prorities Study 研究報告提供了一些有關如何制定特定支出決策的看法。在回答研究問卷的公司中，有 73%的人認為預算支出應該與行業中的最佳實踐（Best Practice）保持一致，這是一個令人鼓舞（即使有些含糊）的回應，表明了做正確事的動機。另一方面，有 66%的人會花一些預算來遵守法律和法規，儘管有人表示這正是政府強制與最佳做法保持一致的方式，但許多企業卻不這樣認為：被調查者表示合規要求是對執行戰略計劃的一種「干擾」。

2019 年最大的支出案例之一是，公司正在決定希望獲得外部網路安全服務的幫助。託管資安服務（Managed Security Services）的範圍從事件回應及支援到提供完整的基礎架構管理：2019年，這些服務的支出達到 642 億美元，是基礎設施保護和網路安全設備投資的兩倍以上。 Kennet Research 估計，此支出在未來四年中將以兩位數的速度增長。

不過，就中小企業資安狀態而言，Kennet Research 也發佈了令人挫敗的消息。在 2019 年針對中小型企業決策者的調查中，有 18% 的人將網路安全視為最低優先事項。這種態度來自一定程度的自滿：66% 的人認為網路攻擊是不太可能的 - 儘管 2019 年有 67% 的中小企業實際上受到了網路攻擊。

資安就業數字

這所有數字之中透露的一則訊息應該會讓資安專家們眼睛一亮：你不可或缺！〈2020 State of the CIO〉的研究報告揭露有 40% 的 IT 領導者認為資安職務最難填滿。這是因為據 ISC2 研究發現，資安專業人員實際上失業率是 0。

挾帶著關鍵性與高需求的雙重優勢，不難想像資訊安全在諸多企業中逐漸掌權。據〈2020 State of the CIO〉研究指出，54% 應答的企業組織在 CXO 高層擁有資安主管，像是 CSO、CISO 等等這類職稱。而且這些資安職務不一定只是從 IT 獨立出來：它們有 40%以上直接向 CEO 報告，而非 CIO 或其他 IT 執行高層。（另一個顯示高階資安專家的需求有多迫切的事實是：這些執行高層中有 25%，已有外部企業組織試圖接觸，努力說服他們離開現有工作。）

這些訊息加總起來，讓資訊安全成了有駭客能力者可以賺錢的職務領域。就在 2020 年初，ZipRescruiter 就將美國入門級資安專家的平均薪資訂在年薪 74,340 美元。（這幾乎是所有入門級職務國家平均水準的兩倍。）更專業的職務還能達到更高薪資：據 Mondo 指出，應用安全工程師每年賺取高達 180,000 美元，而資訊安全管理則一年淨賺 215,000 美元。不同於我們在本文接觸的那許多可怕的數字，這些數字對資安專家們而言應是美妙音符。