美國資訊安全分析新挑戰：巨量資料（Big Data）之應用

在2013年的國際資訊安全會議（RSA Conference）上，資安專家紛紛表示，將Big Data技術應用於資訊安全分析的項目上，確實可以幫助企業建立更佳的情勢判斷能力，但在實際執行過程中是一大挑戰。

資安廠商如RSA和賽門鐵克公司，在會議上表示目前的策略是透過新的數據匯集、比對和分析協助企業篩選、過濾結構化和未結構化資料的威脅指標，這是傳統的特徵偵測（signature-based）安全工具無法做到的。

不像傳統的安全手段著重於阻斷攻擊，新的技術強調偵測並立即回應違犯行為，也就是提前遏止任何違犯行為，協助企業作全面性的偵測而不擔心有所遺漏。

由於越來越多的美國政府機關和民間企業遭受到針對性和持續性的攻擊，巨量資料技術的應用需求激增。企業內部都累積著大量的數據和多元的數據種類，而需要動新技術來保護這些數據資料免於惡意人士或對手的竊取或其他侵害行為。企業應該要因應實際面臨的威脅和所獲悉的威脅情報來建立安全模型，取代部署特定產品和外圍系統的防禦。

美國無論是政府機關或民間企業都被捲入了不對稱戰爭-對手是武器精良、準備充分並有嚴密組織的網路敵人。

「駭客只需要攻擊成功一次，但我們必須每次都是成功的」賽門鐵克的總裁deSouza表示。「因此與其專注的在阻擋所有威脅，更好的辦法是使用巨量資料技術偵測侵入行為並消解之」。而在會議中資安專家都肯認至少從理論上來說，以巨量資料技術強化資訊安全是很好的想法。

不過另有其他的說法，金融服務企業LSQ的首席安全及法務主管皮爾遜認為，許多人的電腦紀錄檔和所有的電子裝置都早就被侵入滲透了，這才是問題所在。他表示，目前現存的SIEM（安全性資訊及事件管理）工具可以讓企業聚集來自許多個安全設備的巨量登錄數據整合在同一系統內，但真正的問題是，SIEM工具必須要有能力分析數據並找出關聯性，如此才能偵測到駭客入侵的前兆證據和真實的入侵行為，這和彙整數據是不同的兩件事。許多企業所面臨的問題不是缺乏數據資料，而是要如何為資訊安全的目的建立關聯規則和應用方式，以有效率的方式找出有用的巨量數據並進行分析，和留下可供進行訴訟使用的證據。

相關連結

Cyclone Interactive, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, Apr. 10, 2013

Jaikumar Vijayan, Applying big data approaches to information security a challenge, Computerworld, Apr. 10, 2013

陳秭璇 編譯整理

上稿時間：2013年04月

資料來源：

Jaikumar Vijayan, Applying big data approaches to information security a challenge, Computerworld, Apr. 10, 2013, http://www.computerworld.com/s/article/9237212/Applying_big_data_approaches_to_information_security_a_challenge_ (last visited Apr. 15, 2013).
Cyclone Interactive, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, Apr. 10, 2013, http://www.emc.com/leadership/digital-universe/iview/information-security-2020.htm (last visited Apr. 15, 2013)

推薦文章