波蘭大學與學研機構竭力反制網路攻擊

駐波蘭代表處教育組

資安業者 Check Point Research 於 2021 年 8 月公布一份報告，說明高等教育及學研機構遭受網路攻擊的情形，數據顯示 2021 年 7 月平均每週發生 2,700 件針對波蘭教育及學研機構的資安攻擊，波蘭科學院一級研究單位資安事故增加，羅茲大學發現嘗試侵入職員電郵信箱駭客活動變多，華沙大學觀察到的網路攻擊頻率並未降低。

波蘭教育學術領域機構成為網路攻擊特定目標，主因為智慧財產的竊取，疫情期間取得重大學術成果的渠道更為重要，攻擊類型包括商業詐騙行為與產業網路間諜。其次為取得大量學生、校友、教研人員的個資，可作為進一步攻擊使用或於黑市販賣。相較於企業與公司，教育學研機構維持網路安全資源有限，更易成為目標。

波蘭教育科學部對此表示未曾接獲教育學術領域的重大網路攻擊事故報告，該部的網路攻擊防護作為向以系統化解決方案為主，確保教育及照護機構執行任務提供教育服務時的資訊安全環境。

波蘭當前威脅分析團隊 CERT 主任 Sebastian Kondraszuk 指出 2020 年處理 10 多件針對大學或研究機構的資安事故，自 2018 年頒布國家網路安全系統法以來，並無觀察到網路犯罪者集中攻擊特定區塊領域的趨勢，而被攻擊者多面對偽造內部單位竊取機敏資訊的釣魚郵件，製造軟體程式錯誤，使資料外洩、系統被入侵或惡意軟體感染。該團隊隸屬於波蘭國家研究機構科學學術電腦運算網絡，專責監控國家層級網路安全威脅與事故。

波蘭科學院已察覺攻擊院內一級研究單位的資安事故漸增，惟尚未掌握自行配有資訊科技設備的其餘院內單位，目前持續更新系統加密資料，善用硬體安全設備及專業級軟體，並重視院外安全監察機制與資安訓練。

羅茲大學發言人 Pawel Spiechowicz 反應嘗試侵入校內員工電郵信箱的攻擊次數增加，多屬於蠻力攻擊（Brute Force），將密碼逐個推算直到找出真正的密碼為止，針對學校服務使用者的釣魚攻擊亦不在少數。校方設置資安解決方案，支持行政部門的硬體基礎設施並更新

防毒系統等關鍵元件，同時持續監測資安系統回傳數據，處理非標準的可疑活動。

華沙大學發言人 Anna Modzelewska 解釋，校方遭受網路攻擊的頻率並未降低，次數與密集度多年維持不變，也承認維持高資安防護等級帶來的挑戰，自 2016 年根據 ISO/IEC27001:2013 規範於校內資安部門設置專責小組，回應網路攻擊。

亞捷隆大學電腦科學中心主任 Lucjan Stalmach 則說據校方觀察，網路攻擊針對職員和學生等終端使用者，瞄準人性弱點，過於逼真的釣魚訊息使收件者難以辨別，不瞭解此種攻擊型態的使用者成為洩露個人帳戶密碼的來源。校方並未放任針對資訊科技系統的攻擊，持續提升虛擬網路的使用安全，強化裝設高階網路安全設備的全校防護網，將更多的學校服務自各學院轉移至學校主控的網路基礎設施（建立在防火牆內的私有雲）。

撰稿人/譯稿人：駐波蘭代表處教育組

資料來源：波蘭通訊社 Polska Agencja Prasowa (2021, August 27)

“Polskie uczelnie i instytucje naukowe zmagają się z cyberatakami”

https://naukawpolsce.pap.pl/aktualnosci/news%2C89064%2Cpolskie-uczelnie-i-instytucje-naukowe-zmagaja-sie-z-cyberatakami.html