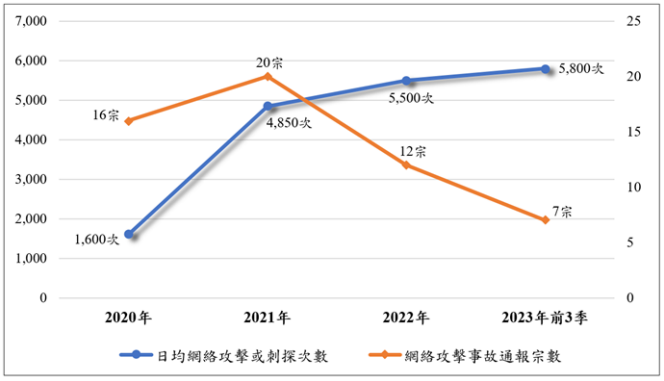
攜手築牢澳門網絡安全防線

《網絡安全法》生效近四年，在網絡安全委員會協調及統籌下，網絡安全事故預警及應急中心、各領域行業的監管實體以及關鍵基礎設施營運者通力合作、各司其職，朝著築牢澳門網絡安全防線之共同目標，有序落實多項網安工作。現時，澳門網安體系順暢運作，各參與方網安意識大幅提升，管理及技術能力不斷進步，整體呈現良好的發展勢頭。然而，本澳網安工作依然面臨著較大挑戰，營運者在技術層面仍然普遍面對若干突出安全威脅，因此各方必須繼續齊心協力，並且透過社會各界支持參與，進一步提升澳門總體的網絡安全水平。

一、風險管控處置水平顯著提升

根據網絡安全事故預警及應急中心（下簡稱“網安中心”）統計，針對本澳關鍵基礎設施的網絡攻擊和刺探數量逐年持續增多，由 2020 年日均 1,850 次（每分鐘約 1.3 次）大幅增加至今年前三季日均 5,800 次（每分鐘約 4 次）。雖然如此，營運者因網絡攻擊而發生的事故並沒有同步增加，反而呈現明顯下降趨勢，從 2021 年的 20 宗大幅減少 4 成至去年共 12 宗，在今年前三季更進一步減至 7 宗。

由此可見，通過網安體系各參與方共同努力，營運者的網安管理和技術能力正持續提升，抵禦網絡攻擊的能力不斷加強，本澳整體網安建設工作呈現良好的發展勢頭。



二、需進一步加強網安防護能力

雖然本澳網安建設呈現良好發展勢頭，惟仍存在網絡攻擊事故偶發的情況，網安中心分析指出關鍵基礎設施營運者仍普遍面對下列三項較為突出的安全威脅：

1) 利用漏洞入侵電腦系統：經網安中心對所有本澳網絡攻擊事故進行取證分析後，發現近七成事故的成因是營運者未有及時發現和修補系統存在的安全漏洞，而被黑客利用實施網絡入侵，繼而進行加密勒索、“挖礦”加密貨幣、竄改網站內容等犯罪行為，甚至利用被入侵的電腦向其他系統發動攻擊。

2) 盜用系統登入帳號：部分營運者由於欠缺完善的帳號安全管理策略，加上用戶安全意識不足，而被黑客透過暴力破解、網絡釣魚等手段，竊取電腦系統用戶帳號的登入密碼，然後盜用帳號向外發送大量病毒電郵、垃圾電郵和不實資訊，或者配合利用有關系統的其他安全漏洞實施網絡入侵。

3) 分散式拒絕服務攻擊：部分營運者由於各種原因，沒有為對外網絡服務配置合適的分散式拒絕服務攻擊（DDoS）防禦措施，導致當受到這類攻擊時，相關網絡服務的穩定運作受嚴重影響甚至癱瘓。

針對上述威脅，網安中心於今年已重點加強網安威脅情報搜集分析能力，以及時和更有效地協助營運者發現安全漏洞、帳號外洩等安全風險，今年底將出台《漏洞管理技術指引》，從而促進營運者提升漏洞管理的技術能力。同時，營運者亦應繼續積極配合特區政府工作，依法履行各項網安義務，持續優化調整相關管理和技術措施，妥善管控各類網安風險。

三、維護網安有賴社會協同參與

面對日益嚴峻的網安形勢，尤其是由專業黑客組織甚至具國家背景的黑客活動構成的嚴重風險，包括營運者在內的網安體系各參與方一刻也不能有所鬆懈，必須始終保持防範意識並持之以恆，根據新形勢、新挑戰、新需求，不斷完善本澳整體的網安建設。在網安委協調及統籌下，網安中心、監管實體及營運者需要一如既往攜手合作，堅持發展與安全並重，持續優化網安運作機制和技術水平，確保各類重要網絡服務安全穩定，助力維護國家安全和澳門社會正常運作。

與此同時，大部分私營企業和社會團體雖不屬《網絡安全法》的規範對象，但同樣面臨網安風險，也是網絡犯罪的侵害目標。因此，社會各界應加緊重視網絡安全，不斷提高安全意識、落實適切保護措施，從而給自身和服務對象提供更佳保障。維護網絡安全是全社會的共同責任，需要政府與社會各界齊心合力、共同參與，攜手築牢澳門網絡安全防線。