事宜：關於立法會梁鴻細議員提出之書面質詢

就立法會透過2022年9月6日第879/E669/VII/GPAL/2022號公函轉來，梁鴻細議員於2022年8月30日提出，行政長官辦公室於2022年9月6日收到之書面質詢，經徵詢司法警察局及行政公職局之意見，本辦公室現回覆如下：

為更好保護本澳關鍵基礎設施營運者的資訊網絡、電腦系統及電腦數據資料，在制度建設方面，澳門特區在2019年制定並實施第13/2019號法律《網絡安全法》，明確規定關鍵基礎設施營運者須履行維護其自身網絡安全狀況的義務和責任，並於2020年5月頒佈《網絡安全—管理基準規範》和《網絡安全—事故預警、應對及通報規範》，以進一步具體規定關鍵基礎設施營運者依照《網絡安全法》須履行各項網安義務的具體措施、程序和要求。同時，在組織保障方面，特區政府於上述法律生效當日（2019年12月22日），依法建立由網絡安全委員會、網絡安全事故預警及應急中心（司法警察局統籌，聯同行政公職局及郵電局組成）及網絡安全監管實體組成的澳門特別行政區網絡安全體系，並逐步形成在網絡安全委員會領導下，網絡安全事故預警及應急中心與監管實體和關鍵基礎設施營運者密切配合的相關工作機制。

根據《網絡安全法》和上述技術規範的要求，本澳各公共部門須制定適當的網絡安全事故應急預案，並從組織和技術層面，落實各項與網絡安全相關的事前預防、事中監察和事後改善工作，從而形成網絡安全管理閉環，以切實保護公共部門電腦系統中包括涉及國家安全的相關資訊。其中，在組織層面，要求須指定網絡安全負責人、制定內部的網絡安全政策和工作指引、為資訊系統和網絡安全工作進行適當的職務分工等；在技術層面，則要求根據各個網絡資訊系統的重要性進行分級，落實相應強度的網絡安全技術措施，包括構建防火牆、入侵偵測及防禦系統、安全網關、及時為軟硬件設備進行安全更新等，以防範外部的黑客攻擊，以及按照“最少權限原則”為員工合理分配系統權限，建立良好的密碼策略和操作日誌審計記錄，以防範內部工作人員越權取存和竄改電腦數據資料等。此外，各公共部門依法須每年對其網絡安全狀況進行風險評估，並向其網絡安全監管實體提交年度報告。

自《網絡安全法》實施以來，本澳相關的網絡安全工作機制持續運作順暢並發揮作用。根據行政公職局提供的資料，本澳各公共部門一直按照《網絡安全法》和上述技術規範的要求開展維護網絡安全的相關工作，特區政府亦有適時跟進及審核各部門相關網絡安全規劃及執行成效，並從中提供相應的技術支援。另外，至今未有發生因公共部門故意違反或不配合履行網安義務，而需要監管實體依法作出處罰的案例。

至於加強人員網絡安全意識方面，行政公職局表示，其持續向不同範疇及職級人員提供相關培訓和工作坊，包括針對實務操作開辦“網絡安全意識教育課程”、“一戶通技術培訓系列課程”等培訓活動，讓負責執行及操作的人員正確使用相關系統，強化網絡安全意識。同時，在技術及管理方面提供“國家註冊信息系統審計師（CISP-A）”、“C.I.S.P註冊信息安全專業人員—澳門認證課程”、“網站應用保安課程”、“網絡安全與業務營運課程”、“電子政務主題工作坊—資訊系統開發及網絡系統管理”等課程，強化相關人員系統開發、維護和運作方面的知識。

此外，網絡安全事故預警及應急中心定期向包括公共部門在內的關鍵基礎設施營運者舉辦各類宣傳教育和專業培訓活動，並且每年舉辦網安事故演習，以提高相關人員的資訊安全管理能力，以及應對突發網安事故的綜合能力。

保安司司長辦公室代主任曾翔

Cheong CHANG
Assinatura digital
2022.09.22 17:13:38 +0800