黑客連環入侵港企業系統 兩大風險須留意

◆簡培欽表示，網絡安全測試就像做新冠快測一樣，需要定期進行測試。 香港文匯報記者涂穴 攝

近月頻頻爆出有香港企業被黑客入侵，在詐騙活動日益猖獗下，企業必須及時掌握不斷變化的網絡安全趨勢和應對存在風險威脅。網絡安全專家、Cyberbay行政總裁及聯合創辦人簡培欽日前接受香港文匯報訪問時表示，中小企目前正面臨兩大網絡安全風險，第一是不少企業從未做過檢測，第二是部分企業不了解正在使用的技術背後有什麼漏洞及弱點，容易被不法分子利用。該公司在香港提供懸賞以協助找尋網絡安全漏洞，他表示，網絡安全測試就像做新冠快測一樣，兩年前做過測試不代表現在同樣安全，所以定期的網絡安全測試是必須的。 ◆香港文匯報記者 黎梓田

中小賞金獵人找網絡漏洞 企要定期快測

◆方保僑表示，網上購物及電子支付日趨頻繁，令不熟悉網絡安全的用戶極容易暴露在風險中。 資料圖片

「香港銳意發展創新科技，惟網絡安全風險仍未得到高度重視，不少中小企業不但無法掌握網絡安全的檢測技術，甚至連配對有合適技術的網絡安全公司也不容易。」他指，該公司在與警務處合作的「守網運動」當中，觀察到有超過八成的參與企業都出現需要馬上改善的漏洞，反映中小企面臨的網絡風險相當高。他形容，網絡安全測試就像做新冠快測一樣，需要定期進行測試。他舉例指，中小企常見的網絡安全風險就是用「罐頭」或「模板」設立網站，網絡安全設定不完善，容易被黑客從該網站上奪取該網站上的賬號及資料。

數據外洩 企業客戶同受損

他進一步指出，中小企另一主要網絡安全風險是數據洩露，例如學歷、個人資料、病歷等。簡指，數據庫「絕對信任」公司網站，會根據網站發出的指示提供資料，如果公司網站設計出現漏洞，就會被不分法子透過網站漏洞奪取數據庫中的資料，造成公司及客戶的損失。很多黑客都會利用OS（作業系統）作為工具，透過任何指令攻擊周邊鄰近網絡系統，而且這些「攻勢」具備「傳染性」，當黑客取得系統的控制權後，就有機會展開大規模的網絡攻擊。

按管理員級別設存取權限

對此，簡培欽建議，中小企不論是自己寫網站又或者用「罐頭」，在建設網站的階段就應該同步進行檢測，確保網站沒有漏洞以及分清楚管理員的級別及存取權限，避免普通用戶也能隨便存取重要資料，從而降低之後修補漏洞所需的成本。他認為，中小企業對於網絡安全檢測最擔心的並不是價錢，而是投入資金後是否能精準找出網絡漏洞。

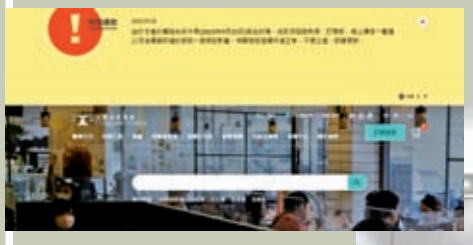
簡培欽表示，這就是他創辦Cyberbay的原因之一。他以自己創立公司為例，Cyberbay在2022年成立時，是香港少見的網絡安全漏洞賞金平台，賞金獵人透過平台接受懸賞任務，尋找並報告網絡漏洞，平台負責為網絡漏洞評級，並按照評級釐定賞金。其後企業可購買網絡漏洞報告並支付賞金，並與網絡安全方案供應商進行一對一諮詢，於漏洞修正後邀請賞金獵人進行重複測試，以確認漏洞的修復情況。平台能有效配對擅長尋找網絡漏洞的賞金獵人，並由熟悉該網絡漏洞的賞金獵人修復漏洞，大大提高中小企投入資金的精準性。

簡培欽認為，香港要把創科事業做到蒸蒸日上，網絡安全重要性不容忽視，他希望賞金獵人日後在香港能成為一個成熟的行業。他表示，香港在賞金獵人行業發展方面現在只是起步階段，慶幸的是已有不少「黑客」人才，目前參與平台的賞金獵人已有一百多人。

近期矚目黑客入侵事件

發生時間	涉事企業/機構	造成後果
10月	Sony	確認遭黑客入侵，近7,000人數據外洩
9月	消委會	約有8,000名人士資料懷疑外洩，包括員工、前員工、職位申請人、《選擇》月刊訂戶及活動投票人等
9月	凱撒娛樂	電腦系統曾遭黑客入侵，相當數量參與忠誠客戶計劃的用戶個人資料外洩
9月	美高梅	造成多個系統癱瘓，包括老虎機、酒店電子鑰匙等
8月	數碼港	超過400GB資料外洩，其中包括初創公司職員的身份證明文件、公司文件、照片等

資料來源：市場消息



◆香港消委會電腦系統曾遭黑客入侵，被盜65GB資料，近80%系統受破壞。 資料圖片

港可疑數碼詐騙率18% 全球最高

隨着消費者和企業持續透過數碼渠道作商業交易，騙徒伺機從中獲利的情況亦日益嚴重。環聯最近發布的全球分析報告顯示，可疑數碼詐騙交易在今年上半年影響遍及各行各業，零售及電子遊戲成為全球最常被攻擊的行業。期內的可疑數碼詐騙交易比率為5.3%，較去年同期上升18%，而全球可疑數碼交易的宗數則上升27%。單計香港的可疑數碼詐騙交易比率更高達18.3%，屬調查所及的市場及地區之中最高，源自香港的數碼交易中，可疑交易的宗數較去年同期大增57%。

零售業詐騙比率最高

在調查所及的所有行業之中，零售業、電子遊戲業及電訊業在今年上半年的全球可疑數碼詐騙交易比率最高，分別為10.6%、7.0%及5.3%。而與博彩業（網上體育博彩、撲克等活動）相關的數碼交易宗數則升幅最多，按年增幅達85%。源自香港的數碼交易方面，旅遊及休閒業和虛擬社區（網上約會、論壇等）於上半年的可疑數碼詐騙交易比率屬調查所及的行業當中最高，分別為8.1%和4.8%。

環聯亞太區首席產品官殷虹表示，衡量數碼詐騙對特定行業的影響時，單純考量詐騙交易比率並不足夠，需要綜合考慮多項因素，如行業的整體規模、是否正在經歷增長及其增長率等。全面分析多項數據方可了解數碼詐騙對該等行業的影響，這更有助預測騙徒未來可能會聚焦的攻擊方向。

逾三成消費者曾成詐騙目標

另外，環聯於7月10至19日期間訪問了973名香港成年消費者，了解他們過去三個月有否成為網絡、電郵、電話或短訊數碼詐騙的目標。該調查發現，32%受訪者表示在過去三個月曾成為可疑數碼詐騙的目標，6%更表示已成為數碼詐騙受害者。當中以語音釣魚（Vishing，即透過詐騙電話誘使他人透露個人資料）為香港受訪者最常遇到的詐騙手法，涉及34%受訪者；其次則為網絡釣魚（Phishing，即透過詐騙電郵、網站、社交帖文及二維碼等盜取資料，佔31%）及短訊釣魚（Smishing，即透過詐騙短訊誘騙他人洩露數據，佔29%）。

殷虹補充，消費者對數碼服務的接受程度不斷上升，加上騷擾電話猖獗，由數碼詐騙引致的損失劇增。消費者較以往更依賴網上平台進行交易的同時，亦更期望企業能保障他們免受詐騙活動的侵擾，並主動辨識可疑賬戶。因此，企業需安排足夠的資源以提升數據分析及技術能力，從而更準確及更有效地辨識潛在的詐騙活動。

「最大風險是不知道有風險」

隨着生活數碼化日益普及，企業或個人的生活或多或少都轉至網上進行，正如處理個人財務資產少不了經互聯網進行，這正好給予騙徒或黑客入侵的機會，網絡安全維護便成了守護市民財產的一道重要防護屏障。網絡安全專家Cyberbay行政總裁及聯合創辦人簡培欽接受訪問時表示，普遍市民或中小企連自己有什麼網絡風險都不清楚，更不用說懂不懂進行網絡安全檢測。他歸納多種網上防騙招式，藉此幫助企業和市民做個「醒目數碼公民」。

檢測費昂貴礙中小企防護

「現在最大問題是大家根本不知道自己面對問題和風險，越不清楚自己有什麼風險，那麼風險就越高」。簡培欽認為，首要做的是網絡安全檢測，問題是相關檢測費用昂貴，令中小企及個人用戶都望而卻步。

他認為，提升大眾對網絡安全的重視，需要有一個「中間人」，而這個「中間人」需要具備全面的網絡安全知識，能將網絡安全技術應用帶給公眾。Cyberbay在向這方向進發，希望透過提供網絡檢測服務，將網絡安全知識及技術帶給中小企及公眾。

他以雲端技術作例子指出，一般網絡保安就好比普通夾萬，而雲端用代碼運行就好比各種形形色色的夾萬，當中有「銀行級數」的夾萬可以選用。一般初接觸雲端的人來說，即使給他「銀行級數」的夾萬也不懂得運用，雲端的問題在於它有「太多選擇」，而網絡檢測的好處就是可以讓用家了解如何正確運用雲端，避免對住「銀行級數」的夾萬卻不懂用。

他又指，個人用戶一般會犯下的錯誤是多個賬號都使用同一個密碼或類似的密碼，因而能輕易被黑客破解密碼並盜取賬號。一般人不知道的是，黑客破解密碼的難度在於其密碼的長度，理論上密碼愈長愈難破解，最好就是11位或以上混合大小寫英文字母、數字及符號的密碼，切勿只使用阿拉伯數字組合的密碼，最好定期更改密碼。

他表示，用戶可以在慣用的密碼組合加上網站、機構名稱或自己能看懂的語言以識別，就能輕易記住。

此外，簡培欽也建議，個人用戶可以瀏覽「have i been pwned」網站，在該網站輸入自己的電郵檢查一下是否曾被洩露資料。如曾被洩露資料，網站會顯示出資料被洩露的日期、被洩露資料的類型，用戶此時應該立即更改密碼以保安全。

方保僑籲安裝正版防病毒軟件

近年智能手機、電腦等數碼產品日益普及，香港資訊科技商會榮譽會長方保僑接受香港文匯報訪問時表示，愈來愈多市民和企業利用不同社交媒體溝通、使用網上購物平台以及電子支付等，這意味有更多不熟悉網絡安全的用戶極容易暴露在風險之中，成為網絡騙徒的目標。

他建議，不論使用電腦和手機都要安裝正版的防病毒軟件及防火牆，並定期更新，以保護自己的電子設備免受惡意軟件侵害。網上交易時應確保網站具有安全認證（例如網站應該是https://），並使用可靠的支付方式，或選擇一些信譽良好的購物網站。

另外，近日社交通訊軟件WhatsApp頻被騙徒用作詐騙的工具，方保僑建議市民在收到網絡訊息時，要留意發送人是否為熟悉的朋友或親人，在點擊連結或下載附件前謹慎核對網址及發送人，以確保來源的真確性，如有懷疑，切勿輕舉妄動。市民如遇上詐騙，應立即停止與對方的對話並報警求助，以有效遏止詐騙案發生，保護自己和他人免招損失。

時刻警惕陌生人訊息

他指，面對變化多端的互聯網，市民愈來愈依賴網上服務，需要時刻提高警惕，採取防範措施。一旦懷疑遇上騙案，應該與執法機關及相關機構聯絡，共同打擊網絡詐騙，以保護自己和他人的網絡安全。

方保僑又指，騙徒利用科技詐騙的手法不斷升級，會利用釣魚網站、虛假社交媒體賬號等。網上詐騙形式亦層出不窮，例如冒充親友並以不同藉口向受害者詐騙金錢、假冒金融機構詐騙等，令人防不勝防。他提議市民應盡量使用複雜的密碼，並定期更改。另外，所有社交媒體賬戶和個人通訊軟件必須開啟兩步認證，以增加賬戶的安全性。