文匯報
WEN WEI PO
www.wenweipo.com
政府指定刊登有關法律廣告之刊物
獲特許可在全國各地發行
2018年4月19日 星期四
大致多雲 午後明朗
戊戌年三月初四 初五穀雨 氣溫22–26℃ 濕度70–90%
港字第24870 今日出紙3疊10大張 港售8元

香港寬頻被黑 疑洩38萬客私隱

停用伺服器遭入侵 內有4.3萬信用卡資料

香港文匯報訊（記者 吳子晴）香港寬頻有限公司昨日公佈，集團一個已停用的資料庫伺服器遭身份不明者入侵，該資料庫涉及至2012年約38萬條固網電話及IDD服務客戶申請人記錄，包括其個人資料及約4.3萬條信用卡資料，受影響資料佔整體客戶記錄的11%。香港寬頻已向警方報案，並將通知受影響客戶及個人資料私隱專員，又指已採取即時措施防止日後遭受任何類似攻擊。有資訊保安專家表示，相信事件是疏忽所致，認為香港寬頻有責任將涉事的資料庫加密。

香港寬頻於昨日收市後發公告指，於本月16日，集團發現一宗未經授權接觸其一個已停用客戶資料庫的事件。該資料庫包括集團截至2012年約38萬條固定及IDD服務客戶及服務申請人記錄，約佔其360萬條客戶記錄的11%。

報警處理並通知相關客戶

這些截至2012年的資料包括姓名、電郵地址、通訊地址、電話號碼、身份證號碼及約4.3萬條信用卡資料。集團已立即進行徹底的內部調查，並聘請外部網絡安全顧問對所有系統及伺服器進行全面檢查，以防止日後任何類似攻擊。

香港寬頻表示非常重視此事件，並已立即向香港警務處報告上述事件，並將通知受影響的客戶及就此通知香港個人資料私隱專員。香港寬頻表示，將在此過程中與有關部門合作，打擊此等違法行為。

該公司在聲明中指出：「本集團已採取即時措施以防止日後任何類似攻擊。本集團並不知悉本集團任何其他客戶資料庫受到影響。本公司相信此為一宗獨立事件，且不會對本集團的業務及營運造成任何重大影響。」

發言人指黑客技術「超前」

香港寬頻發言人指，目前調查所得，是次並非普通黑客所為，是以超前技術入侵，呼籲客戶留意可疑信息及信用卡賬單。香港寬頻表示，客戶查詢可致電36169111或電郵至inquiry_36169111@hkbn.net。

私隱專員對事件表示關注，由於涉及客戶人數眾多，已主動展開循規審查。商務及經濟發展局局長邱騰華表示，已知悉事件，並知道香港寬頻已報警，相信警方會調查。

專家：相信事涉保安疏忽

香港資訊科技商會榮譽會長方保僑對香港文匯報表示，香港寬頻作為互聯網供應商，網絡技術應較超前，今次出現疑似黑客入侵事件，相信涉及資料保安漏洞或疏忽。

由於事件中的已停用客戶資料庫的資料並無加密，他認為當公司處理客戶資料時，無論新或舊的客戶資料，公司都有責任將資料加密，即使黑客取得資料，亦無法瀏覽有關內容。

方保僑建議，如客戶發現資料被盜，客戶如以自己的電話號碼等的個人資料用作網上支付等平台的密碼，便應馬上更改密碼，以免出現不必要的損失。

■香港寬頻昨日發佈消息稱，集團一個已停用的資料庫伺服器遭身份不明者入侵，涉及約38萬個客戶記錄，其中包括約4.3萬條信用卡資料。 中通社

私隱專員：事關多人 即時調查


■私隱專員黃繼兒表示，將就香港寬頻事件展開調查。

特稿

香港寬頻一個已停用的客戶資料庫遭入侵，香港個人資料私隱專員黃繼兒表示，注意到事件中受影響客戶人數眾多，可能涉及大量敏感個人資料，公署已主動就事件展開循規審查。

香港寬頻發言人回覆傳媒查詢時指，因稅務需要，所有舊客戶資料會在後端系統封存7年後才銷毀。

依條例須刪除已停用個人資料

黃繼兒表示，公署已收到香港寬頻相關的資料外洩通報，指該客戶資料庫，載有的客戶資料包括姓名、電郵地址、通訊地址、電話號碼、身份證號碼及信用卡資料等，有可能導致個人資料外洩。

他續說，無論公私營機構，作為資料使用者，必須按《個人資料（私隱）條例》規定妥善儲存客戶的個人資料，並採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用，否則便有可能違反條例下的資料保安原則 。

黃繼兒指出，一般而言，任何機構必須按《私隱條例》的規定妥善保留及刪除客戶的個人資料，包括確保個人資料的保留時間不得超過達至原來目的的實際所需、刪除已不再為使用目的而需要保留的個人資料等。機構應按其業務的實際所需、其收集個人資料的原來目的，以及為符合其他法定要求或公眾利益而決定保存個人資料的期限。

在個人資料轉移方面，黃繼兒表示，當機構在結業/終止業務時擬將該機構的客戶資料轉移予另一提供類似服務的公司時，機構要在轉移客戶的個人資料前已取得客戶自願給予的明示同意，或在收集客戶的個人資料之時，已明確告知客戶收集其個人資料的目的及其個人資料可能被轉移予該指定類別的人士，方能這樣做。

香港寬頻稱客戶資料需封存7年

香港寬頻發言人在回覆傳媒查詢時指，客戶中止公司服務6個月期間，職員可以透過系統，查找客戶資料以展開收回器材等後續工作。因為稅務需要，所有舊客戶資料會在後端系統封存7年後才銷毀，並設有查閱權限，一般職員是沒法接觸。至於是次受影響的客戶資料庫，最舊一批的客戶資料是2012年。

■香港文匯報記者 尹妮

網絡安全公司：港法律欠嚴謹

專家意見

香港寬頻一個儲存已停用資料庫的伺服器遭黑客入侵，涉及38萬條客戶記錄被盜取，包括客戶姓名及信用卡號碼。有網絡安全公司表示，香港的網絡安全監管不足，法例不夠嚴謹，令機構較少留意保安系統的漏洞。

網絡安全公司FireEye銷售工程師王潤霖向香港文匯報表示，由於香港並無法律規管機構當洩露客戶資料時，必須對外公佈，只有指引列明，當洩露大量客戶資料時，才需將事件公佈。他認為，香港的法例不夠嚴謹，機構較少會關注網絡安全問題。

港安全指引多無強迫性

王潤霖認為，香港的機構目前主要集中於系統的防護，而較少投放資源於偵查或調查黑客入侵。在是次事件中可見，香港寬頻須聘請外部網絡安全顧問，反映香港的機構未必有能力偵查黑客問題。再者，事件涉及的是一個已停用的資料庫，大多機構亦不會投放資源於此類伺服器。

他指出，香港於網絡安全的法例比外國落後，有關指引並無強迫性，由於香港主張自由營商，如增加監管，會令營商成本增加。但他認為政府應增加對網絡安全的監管，以保障市民的私隱，增加對市民的保障。

■香港文匯報記者 吳子晴

亞太機構測黑客耗時多4倍


■網絡安全公司FireEye亞太區首席技術總監Bryce Boland。

香港文匯報訊（記者 吳子晴）全球網絡安全問題受到關注，網絡安全公司FireEye昨日發表「M-Trend 2018」研究報告，發現亞太區機構偵測網絡入侵者所需時間中位數為498天，較全球數字高出近4倍。一旦機構受到網絡入侵者攻擊，則有更大可能再次成為攻擊目標，其中金融機構及電信機構為主要入侵目標。FireEye亞太區首席技術總監Bryce Boland表示，各機構需提升網絡安全，不能只停留在守法及合規的層面。

報告發現，亞太區網絡入侵者成功潛伏於系統內時間中位數為498天，較全球中位數101天，高出近4倍。

Bryce Boland指，偵測時間過長，入侵者便有足夠時間得到他們所需的資料。

被侵企業四成為金融機構

他續說，即使政府針對網絡入侵者立法，但立法速度慢，遠追不上網絡入侵者的改變速度，而且機構通常在遭受入侵後，才會正視問題，令亞太區機構偵測網絡入侵者需時較長。

Bryce Boland指出，超過91%曾被攻擊一次或以上的亞太區機構，會再次成為相同或有類似動機的網絡入侵組織的目標。其中，有82%的機構更發現多個網絡攻擊者。

被入侵的機構中有39%為金融機構，而電信機構更是網絡入侵組織的主要入侵目標，因為電信機構掌握大量客戶及交易資料，讓犯罪分子可能從中獲取金錢，而有國家亦可能會入侵其他國家或地區的電信機構，從而取得其他國家或地區的資訊。

Bryce Boland建議各機構必須認清潛在黑客，洞悉攻擊者常用的技巧，了解公司在網絡危機偵測及回應攻擊方面的能力，才能有效地運用其保安資源。公司必須制定策略方針，應付所面對的網絡攻擊威脅。

雲報紙 Android 文匯網 早安香港 Apple iOS 文匯報微信

手按照習近平講話精神 打造世界級城市群

各界獻力共建灣區

詳刊 A2

督印：香港文匯報有限公司 地址：香港仔田灣海旁道7號興偉中心2–4樓 電話：28738288 傳真：28730657 採訪部：28738260 傳真：28731451 廣告部：28739888 傳真：28730009 承印：三友印務有限公司 地址：香港仔田灣海旁道7號興偉中心2–3樓