機密維護案例之電話滲透

壹、真實案例

曾在美國國家安全局擔任安全顧問的伊拉在其所出版的「大盜入侵」一書中，詳實地紀錄他如何入侵企業，並且以電話滲透某知名金融機構，成功獲取到敏感資料的經驗，伊拉真實的案例是這樣的：

伊拉的工作，主要就在於各大企業進行安全滲透測試。首先他選定了一家大型金融機構，藉由網路查詢到該金融機構的相關資訊，並透過電話簿查到該金融機構在當地的辦事處，而伊拉就在當地的辦事處順手取得該金融機構的年報及總公司內部部門的電話。

從年報中，找到該金融機構中許多主管與員工的姓名，然後再由網路搜尋功能查到這些人員的歷史新聞資料。從中選定一位主管，並且冒充該金融機構公關部門的人，打電話給這名主管的秘書，以欲在公司的刊物上報導這名主管的優異表現為由，和秘書小姐閒聊了起來。慢慢地秘書小姐也失去了戒心，在沒有防備的情況下，她告訴了伊拉這名主管的一些私人資料，包括家中成員及興趣嗜好等等。

伊拉又偽裝成該名主管，打電話給各部門秘書，要求他們寄一份員工電話簿給下游承包商（也就是伊拉），沒有多久，伊拉就收到一本本嶄新的電話簿，而裡面包含了所有員工的姓名，以及聯絡電話。

伊拉到此可說已經滲透成功了，但他還不死心，他想進一步了解該金融機構還有沒有哪些漏洞，於是他決定進入該

單位的電腦系統裡，但先決條件是要獲得網路帳號的使用者識別碼與密碼。

伊拉選定新進人員做為下手的目標，他認為新進人員最沒有戒心，而且剛進公司對公司環境和其他人員也不大熟悉。伊拉打電話到新進人員管理部門，偽稱是某高階主管的助理，因為主管要親自歡迎新進人員，需要新進人員名單，恰巧該部門負責人不在，而接電話的又是新進的辦事員，新辦事員二話不說就答應了，半小時後就把新進人員名單 mail 到伊拉的電子信箱裡。

伊拉一個一個打電話給這些新進員工，告訴他要實施有關電腦安全方面的訓練，但需要員工的電腦型式、系統名稱，以及使用者的識別碼與密碼，而在套取密碼的過程中，伊拉會先問些基本問題，然後再告訴他們一些簡單的安全規則，就這樣伊拉輕而易舉地突破了該金融機構的安全防護系統，順利地侵入該單位。

貳、經驗教訓

（一）這個案例告訴我們，不管在任何的情況下，都應該嚴守秘密。事實上，「保守業務機密」不只對國家政府是重要的，對一般的企業機構更是重要；從案例中可以看的出來，新進人員因為對單位不熟悉，再加上缺乏警覺性，結果伊拉只經由電話就套取出個人的識別碼與密碼，而讓伊拉輕易地滲入公司電腦系統裡，還好伊拉只為測試工作需要，如果他是一名間諜，該金融機構將可能造成嚴重的傷害。

（二）其次，伊拉只藉由電話便一層層地入侵金融機構

內部，不但獲得員工的電話簿，還得知高階主管的一些私人資料，以及新進人員的識別碼與密碼。由此可見，電話滲透是無孔不入的，它不需要浪費太多的人力，也不需要大筆的金錢，只要有一張嘴巴，就可能造成對國家政府或是企業機構的危害，這也難怪簡訊、電話詐騙案層出不窮，即使政府、警政機關一再宣傳，還是無法有效遏阻，詐騙案仍是一而再、再而三地發生。

（三）上述的案例，我們應引以為借鏡，除在個人工作崗位上戮力以赴外，在接獲陌生電話，或是與他人閒聊時，都應隨時養成保密的習性，並謹守個人本分，否則一旦業務上應保守的機密或是個人資料外洩，影響的不只是個人本身而已，更可能造成公司莫大的傷害。須知「謹言慎行莫大意，快意多嘴禍害多」，大家都應該謹慎小心才是！

資料來源:法務部廉政署

資料日期:111/06/07