BEC詐騙？帶給企業的損失已然超越勒索軟體和惡意程式

隨著網路的崛起，不管是私人或企業都越來越脫離不了網路興起所伴隨的威脅。從去年台積電機台感染變種病毒引發大規模停擺事件到今年的各式勒索軟體&惡意木馬攻擊案件，駭客無不在更新其手段來威脅、攻擊企業。目前多數企業對於Dos攻擊、勒索軟體&惡意程式攻擊皆有充分了解，並導入各種機制來防護、抵禦，但根據美國FBI網路犯罪申訴中心的一項報告來看，「BEC詐騙」所造成的企業損失遠多過於其他所有攻擊模式，顯然BEC詐騙的投資報酬率是非常高的，且有急速增長的趨勢。

1
鎖定目標
匯款作業相關人員
如：會計、高階主管等

2
惡意程式攻擊
利用釣魚網站或病毒
來引誘受害者上當

3
盜取帳密
拿到信箱密碼後
便可等待時機下手

4
BEC詐騙開始
冒充成廠商或財會人員進行詐騙

台中總公司 04-2705-0888
台中市西屯區西屯路二段256巷6號3F-6

台北分公司 02-2501-1185
台北市中山區松江路129號6F-2

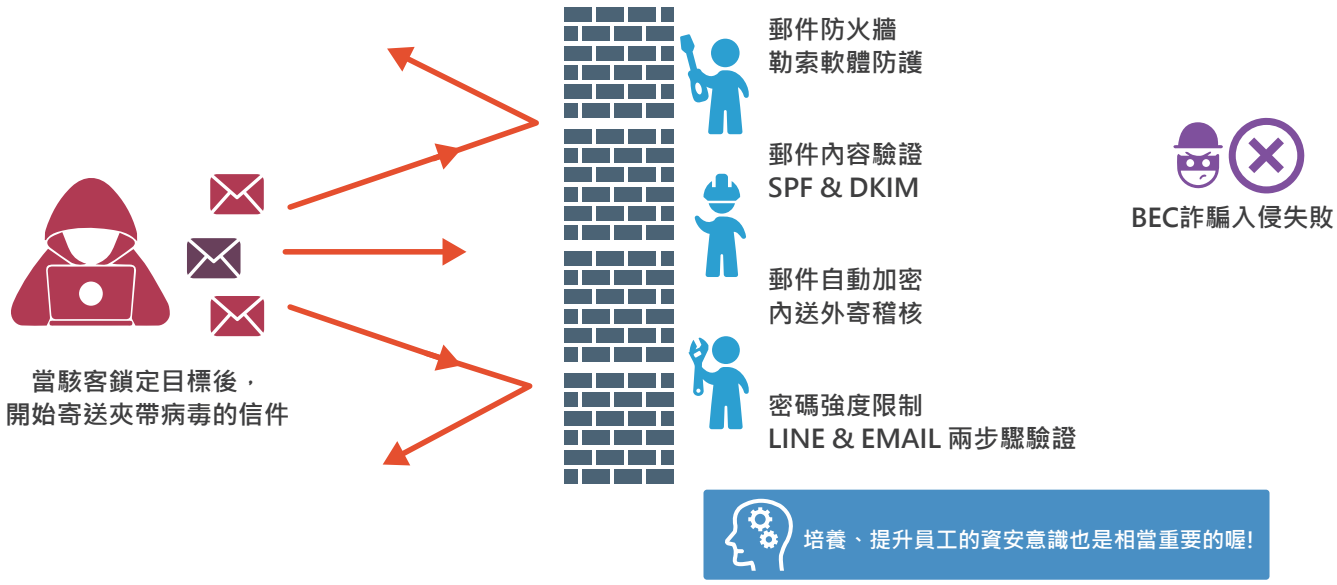
高雄分公司 07-229-8788
高雄市新興區民權一路251號8F-6

免付費專線 0800-666-188

官方網站 | www.sharetech.com.tw
銷售諮詢 | sales@sharetech.com.tw
技術支援 | help@sharetech.com.tw

BEC詐騙？帶給企業的損失已然超越勒索軟體和惡意程式

什麼是BEC詐騙呢？BEC原名為「Business Email Compromise」，中文譯為商業電子郵件詐騙，即透過鎖定企業內特定人員，如：財務會計或高階主管，利用可竊取帳密的釣魚網站或寄送帶有惡意木馬或病毒的郵件誘騙受害者上當後，竊取其信箱帳密，並等待合適的時機來臨，提出以假亂真的匯款請求，如：更改匯款帳戶等。



眾至是如何協助企業打贏名為BEC詐騙的戰爭呢？讓我們一一來解析以下四道防線。

第一道防線--郵件防火牆、勒索軟體防護

透過異常寄送偵測、SMTP流量異常偵測等機制，過濾傳統防火牆無法攔截的大宗郵件攻擊、木馬程式&駭客攻擊等，並依據來源IP和寄件者進行封鎖，針對SMTP(S)、POP3(S)、IMAP(S)等驗證執行攔截，阻止大量試圖破解帳密的情形發生；內建的郵件內文連結資料庫，則可有效阻擋惡意連結。獨特Sandstorm惡意程式過濾，能偵測未知的進階惡意程式附檔，如常見Word、Excel、Power Point或PDF等，若還是覺得不夠安心，也可加購卡巴斯基防毒軟體，為企業的郵件安全再附上一道枷鎖。

第二道防線--郵件內容驗證、SPF&DKIM

專屬郵件安全簽章，讓收件者以信件中的連結與寄件者的郵件主機確認原始郵件內容，降低信件被竄改的風險；SPF能抵擋非法主機偽造合法網域寄出的信件，過濾寄件者網域或來源IP；DKIM網域驗證則用來防止郵件內容遭到竄改。

第三道防線--郵件壓縮加密、內送外寄稽核

萬一信箱不幸地被盜用，藉由自動加密重要信件以及其附檔讓有心人士無法得知信件的內容；再者，針對內寄或外送的郵件主旨、內容中的關鍵字進行審核，對符合設定的郵件實施隔離、刪除、發送通知信、抄送副本等動作，防止重要信件在不知不覺中洩漏出去。

第四道防線--密碼強度限制、帳號登入安全

為防止員工圖方便設置過於簡單的密碼，管理介面中可指定密碼強度限制如須包含大寫英文、符號或長度須超過多少字元；再者，在個人信箱設定介面中可開啟兩步驟驗證，即使密碼被盜竊，藉由LINE或EMAIL就能及時告知並驗證，依然可確保帳戶安全性，若是信箱有異常登入的情形發生，系統也會寄送通知信警示使用者須注意其信箱安全。

隱形的防線--培養員工資安意識，不亂點來路不明的連結、定期變更密碼

其實BEC詐騙的最大特徵是利用人們對於電子郵件的普遍信任，沒有習慣二次確認寄件者是否為當事人，因此對於員工的資安意識教育是非常重要的，如：不隨便亂點來路不明的連結或網站、定期的更改信箱密碼等；眾至也提供企業社交演練，以幾乎真實的狀況模擬讓員工熟悉當遇到BEC詐騙時該如何處理，另外面對日新月異的駭客攻擊手法，我們也透過定期的系統更新來及時應對，以不變應萬變。眾至以20餘年在郵件安全領域的專業度，跟著企業一起面對網路上的各種犯罪活動。