TLP:WHITE

企業客戶資料遭竊的連鎖效應

Announcement Advisory Report（ANAR）

2017-11-15

TWCERTCC-ANAR-2017011

Summary

- 在台灣，有許多小型企業的電子商務平台，其線上購物網站普遍委託網站開發廠商建置，企業對於系統架構與網站設計皆無法掌握，易忽略其網站之資訊安全。
- 電商平台的購物網站，容易成為駭客攻擊的目標，客戶資料經常包含電子郵件帳號、信用卡資料、身分證字號、姓名、生日、地址、電話、購物資訊及金融機構帳戶等，一旦遭駭客竊取客戶資料後，將引發有心人士後續包括惡意郵件寄送、行銷、詐騙或非法信用卡交易等的連鎖效應。

Description

資料外洩成為全球企業的主要資安威脅，根據英國標準協會(British Standards Institution, BSI)的地平線掃描報告[1]表示，在 2017 年全球 10 大營運威脅中，資料外洩所造成的資安風險高居第二。其中台灣在 2017 年亦頻傳企業的客戶資料遭駭客竊取，包含了旅遊業者[2][3][4]、電商業者[5]等，導致其客戶的個人資料、交易紀錄等資訊遭詐騙集團掌握後，利用正確的資料取得受害者信任，再從中誘導受害者進行轉帳來詐取金錢。在電子商務蓬勃發展的時代，企業必須正視客戶資料的保護，以防遭駭客竊取。

台灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team / Coordination Center, TWCERT/CC)在 2017 年 10 月接獲企業通報，表示該企業的線上購物客戶，在近數月間頻頻收到詐騙電話，以明確的個人資料及購買商品的資訊，說服顧客重新轉帳匯款。詐騙集團在取得受害者信任後，便誘騙受害者至 ATM 操作，將款項匯款至指定帳戶中，目前已有 3 名顧客受害。

雖該企業已於刑事警察局立案，但因該企業對資安問題與技術不了解，故請求 TWCERT/CC 配合刑事警察局人員赴現場了解詳情，並協助分析其購物網站內的顧客交易資料外洩的可能原因。經 TWCERT/CC 協處分析後，相關資訊如下：

1. 該受駭購物網站係架設於向服務商所租賃的雲端空間中，相關的連線機制並未採用 SSL 加密機制。
2. 該購物網站的網頁應用程式為委外廠商進行設計與開發，經本中心檢測後，該網頁應用程式存在多個高風險的安全問題，如圖 1 所示。

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	74
High	42
Medium	6
Low	23
Informational	3

圖 1. 網站安全檢測結果

3. 其網路購物作業流程，分別為客戶下單階段、資料匯入階段及揀貨作業階段，如圖 2 所示。

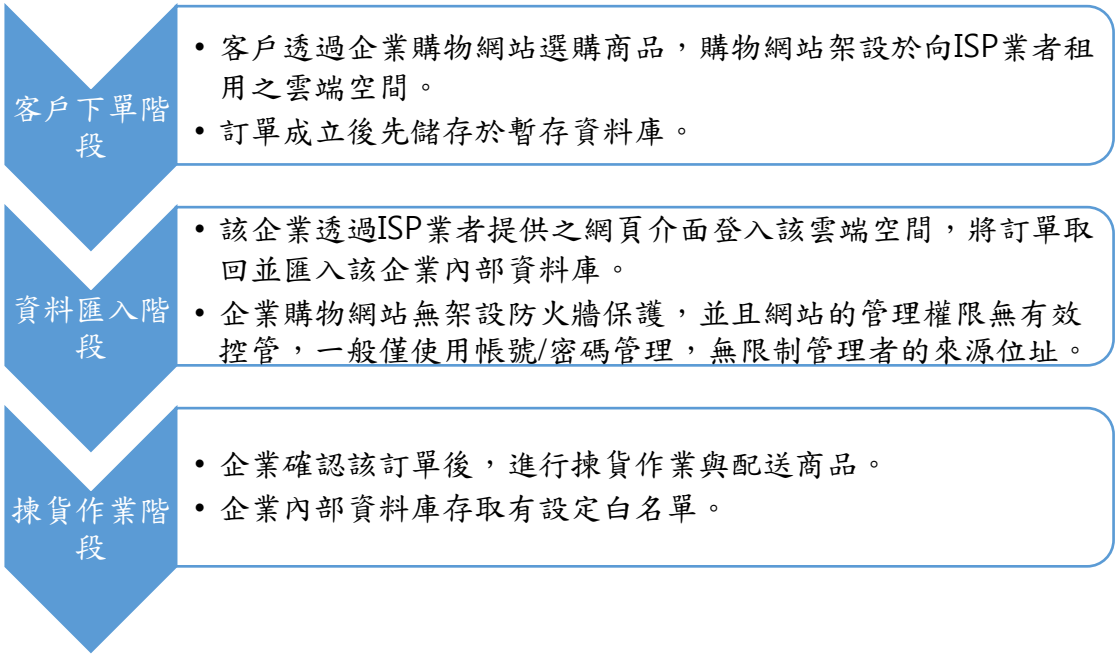

圖 2. 網路購物作業流程

4. 經分析，在購物流中的客戶下單階段，客戶訂單資料已被詐騙集團掌握，包含訂購時間、訂購項目、訂購金額、訂購人名及付款方式等，詐騙集團透過電話假冒該企業，誘騙被害者進行 ATM 轉帳作業，因此研判可能在網站或暫存資料庫端存在漏洞，讓駭客有機可乘。

台灣許多具實體店面的小型企業，因網路的發達與許多網路行銷的成功案例，故有愈來愈多的小型企業也希望讓產品銷售管道多元化，都想透過網路進行販售，然而受限於產業規模與型態，企業員工通常不具資訊及資安相關背景，因此其線上購物網站普遍委託網站開發廠商建置，企業對於系統架構與網站設計皆無法掌

握，開發商因人力、技術及成本考量，相關的安全測試與檢查常被忽略，因此小型企業的電商購物網站普遍存在以下問題：

1. 網站原始碼存在安全漏洞。
2. 網站伺服器的作業系統及應用程式未安全更新至最新版。
3. 網站無防火牆保護或防火牆設定為預設值或設定不正確。
4. 防毒軟體未安裝或未更新至最新病毒碼。
5. 網站資料庫存取未即時監控異常連線。
6. 網站未採用 SSL 加密機制。
7. 網站的管理權限無有效的控管，一般僅使用帳號/密碼管理，無限制管理者的來源。
8. 相同網站開發商所建置之網站，可能使用相同開發框架，若網站開發商對於網站資訊安全不重視，容易導致企業遭遇類似的資安風險。

這樣資安防護薄弱的購物網站，容易成為駭客攻擊的目標，讓駭客可以輕易的取得企業客戶的敏感資料，例如：電子郵件帳號、信用卡資料、身分證字號、姓名、生日、地址、電話、購物資訊及金融機構帳戶資訊等。一旦客戶資料遭駭客竊取後，將引發有心人士後續包括惡意郵件寄送、行銷、詐騙或非法信用卡交易等的連鎖效應，如下：

1. 姓名、生日、地址、電話或購物資訊等個人資料：可販售給其他業者行銷或詐騙集團使用。
2. 電子郵件帳號：可用來申請假帳號、寄發垃圾郵件、釣魚郵件等。
3. 信用卡、金融機構帳戶資訊：可用來線上購物盜刷與付款。

針對電商網站之資安防護，TWCERT/CC 提供以下 6 個防護策略參考：

1. 購物網站的開發時，應要求開發商須納入源碼檢測、弱點掃描及滲透測試等安全軟體發展流程(Secure Software Development Life Cycle, SSDLC)。
2. 網站伺服器的作業系統及應用程式務必安裝最新版的安全更新。
3. 防火牆與防毒軟體需安裝，防火牆規則設定需正確，並常常檢視紀錄，防毒軟體須保持病毒碼可即時更新的設定，並檢視更新是否正常。
4. 網站若涉及企業客戶交易紀錄、客戶資料等，務必採用 SSL 加密機制傳輸敏感資訊。
5. 網站的管理者來源位址需固定，並使用安全的認證方式。
6. 導入資料外洩防護方案(Data Lost Prevention, DLP)，以確保重要資料外流時能即時偵測與攔截，及重要檔案不會在未被授權的環境下被打開而造成資料外洩。

根據台灣法務部頒布的個人資料保護法規定[6]，若企業意外洩漏客戶個資，雖無刑事責任，但仍有民事賠償及行政裁罰責任[7]，企業發展電子商務時切勿忽略網站的資安風險，而導致客戶個人資料遭竊，除可能遭裁罰外，亦可能降低客戶對該企業之信賴感，因而影響企業的營運。

TWCERT/CC 肩負國內民間資安意識與素養的宣導推廣之責任，除在官方網站、官方臉書專頁發布資安資訊外，亦積極透過舉辦研討會、說明會及設攤位方式，向民間及企業推廣資安的重要性，以期提升台灣民間整體資安意識。

References

[1] 英國標準協會, Mar. 17, 2017, "地平線掃描報告", Retrieved Nov. 16, 2017, from the World Wide Web: https://www.bsigroup.com/zh-TW/about-bsi/media-centre/press-release/2017-/march/Horizon-Scan-Report/

[2] TVBS NEWS, Apr. 23, 2017 "可樂旅遊遭駭個資外洩會員被詐騙", Retrieved Nov. 16, 2017, from the World Wide Web: https://news.tvbs.com.tw/local/722374

[3] 聯合新聞網, May 24, 2017 "雄獅旅行個資外洩 民眾遭詐騙近 20 萬元", Retrieved Nov. 16, 2017, from the World Wide Web: https://udn.com/news/story/7320/2482949

[4] 三立新聞網, Oct. 3, 2017 "百威旅遊資料外洩！11 人遭詐騙 最高金額 88 萬", Retrieved Nov. 16, 2017, from the World Wide Web: http://www.setn.com/News.aspx?NewsID=300920

[5] 聯合新聞網, Oct. 14, 2017 "注意！三民書局會員資料外洩 詐騙集團騙了 108 人", Retrieved Nov. 16, 2017, from the World Wide Web: https://udn.com/news/story/7320/2482949

[6] 全國法規資料庫, Dec. 30, 2015 "個人資料保護法", Retrieved Nov. 16, 2017, from the World Wide Web: http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

[7] 自由時報, May 29, 2015 "丹堤咖啡遇「駭」 會員個資全暴露", Retrieved Nov. 20, 2017, from the World Wide Web: http://news.ltn.com.tw/news/society/paper/884533

聯繫資訊

台灣電腦網路危機處理暨協調中心

- 免付費專線：0800-885-066
- 資安事件通報 03-4115387 或 02-23776418
- 電子郵件：twcert@cert.org.tw
- 官方網站：https://www.twcert.org.tw/
- Facebook: http://www.facebook.com/twcertcc