TLP:WHITE

資安通報的挑戰與對策

Announcement Advisory Report（ANAR）

2018-1-10

TWCERTCC-ANAR-2018001

Summary

- 依據 TWCERT/CC 通報與協處經驗，資安通報業務所面對之挑戰主要在於大部分民間企業與民眾資安意識認知不足及法規限制等問題，一般認為所收到的資安通報情資尚未造成其損失，亦無法可強制要求其改善，故對本中心的資安通報常以消極態度因應。

- 鑒於上述之因素，造成本中心在處理資安事件通報作業時常出現滯礙，TWCERT/CC 提出相對之因應對策，期使企業及民眾了解資安通報的用意，以提升其資安意識及完善我國資安通報程序。

Description

駭客針對一般民眾上網習慣，常將熱門新聞議題、關鍵字或影片等民眾有興趣的內容，利用社交網站、即時通訊軟體或電子郵件等管道散布惡意程式或釣魚網站連結。因現階段台灣民眾資安意識仍薄弱，即便瀏覽器或防毒軟體已針對相關可疑網路行為提出警告，仍有民眾不以為意，繼續其網路瀏覽作業。因一般民眾較重視資訊的「獲得」，不在意資訊來源是否「安全」，且普遍有「電腦中毒沒關係，只要移除或重灌，問題就可解決了」的觀念。雖然，表面上看起來問題已被「解決了」，但是實際上問題產生的原因並未被排除，一般民眾不會細究發生資安事件的背後原因，並尋求正確的解決方式，導致相同資安事件重複發生。

TWCERT/CC 在接獲來自國內外的資安通報後，經確認受駭單位為我國企業或民眾，TWCERT/CC 將直接聯繫受駭單位進行資安事件通報，並依事件影響程度協助處理。常見接獲通報之單位對於通報之案件多以不處理、或僅以表面排除等消極態度因應。常因該單位未澈底解決問題而再次出現類似的資安問題，甚至部分單位對 TWCERT/CC 執行通報業務及所通報的內容存疑，而將通報資訊歸類為詐騙集團訊息或垃圾郵件，以致駭侵事件資訊無法即時傳遞給受害單位進行早期處理，可能造成後續重大的損失。

資安事件能否儘快排除，減少損失，主要的關鍵在於事件通報與應處程序能否順利推動，TWCERT/CC 在執行資安事件通報與協處業務上所遇到的問題大致可區分為「資安意識不足」以及「法規的限制」等兩大類別，常見狀況列舉如下。

一、 資安意識不足

1. 對資安事件可能造成危害的嚴重性認知不足

企業或民眾於接獲資安通報後，常因相關資安問題尚未造成其損失，

而對事件排除之處置態度不積極(如程式修訂或系統漏洞修補等)。

例如：針對企業網站遭置換之資安通報(如揭露於 zone-h 或被通報為釣魚網頁)，常見受駭單位僅以移除遭置換的網頁因應，未細究網頁遭換之原因(如對系統進行完整安全檢測)，導致本中心再次接獲該單位網頁被置換之情資。

2. 資訊與資安能力不足，以致無能力修正系統的資安問題

大部分中小企業的網站係委託軟體開發商建置，企業本身對系統架構與設計並無掌握及不了解，另軟體開發商因人力、技術及成本考量，系統安全測試與檢查常被忽略。因此，在接獲資安事件通報時，即使 TWCERT/CC 已於通報資訊中提供處置建議，企業亦無能力處理或無法確認委託商處理狀況。

例如：TWCERT/CC 通報案例中，有許多小型企業由實體店面跨足網路商店，其線上購物網站普遍委託軟體開發廠商建置。當接獲資安通報時，常因系統建置完成後，開發商已無責任，而無法立即協助修訂，導致問題排除時間延長，甚或因該問題尚未造成企業立即的損失，而不修正。

3. 不知道系統需要安全更新或修補系統漏洞，導致資安事件發生

一般企業或民眾因資訊能力或資安意識不足，不了解安全更新是資安防護的重要工作。絕大多數的駭侵事件起源於系統漏洞遭到駭客利用，其中大部分的攻擊是來自於已知的漏洞，而非零時差攻擊[1]。另因企業或民眾所建置之系統對於舊環境或元件相依性重，擔心修補更新後會造成原系統不穩定或損壞[2]，而對資安通報所述之漏洞問題未及時修補或更新意願不高。

例如：2017 年 5 月全球發生 WannaCry 勒索軟體，即是透過微軟已於 3 月公告的漏洞進行攻擊[3]，若用戶能及時修補這個漏洞，相信將可降低該事件的攻擊風險。

4. 不知道發生資安事件應該通報，並可尋求協助

國內一般企業與民眾普遍對資安通報與協處資訊認知不足，目前尚存有家醜不外揚觀念，對於本身遭受資安事件時，大部分民眾僅以重新安裝作業系統的方式處理，而非找出資安事件原因，另外同時也輕忽網路上所發生的資安事件，因而錯失早期防護的時機，導致類似資安事件重複發生。

針對資安意識不足而造成資安通報與協處程序的挑戰，TWCERT/CC 建議之改善對應策略如下：

1. 強調資安通報等級及資安事件影響程度

為使企業或民眾明瞭相關單位所通報資安事件的嚴重性，通報內容可強調事件的影響等級及分級標準資訊，並提供該資安事件相關新聞與參考資料。

2. 鼓勵企業開發軟體時，納入安全軟體發展流程

企業的資訊系統開發過程中，應要求開發人員納入源碼檢測、弱點掃描及滲透測試等安全軟體發展流程(Secure Software Development Life Cycle, SSDLC) [4]。若需委外廠商開發時，除了考量開發成本外，也應將資安檢測納入驗收條件，並建議找資安信譽優良的廠商合作，以免因小失大，影響企業商譽。

3. 提供有效解決方案建議

企業及民眾除了注意漏洞修補、更新程式相關取得管道或問題緩解資訊外，也應確認解決方案之相容性問題。

另可建議進行漏洞修補前置測試，例如，將修補程式安裝於備援系統中運行，以確認修補程式的安裝不會對正式系統造成任何非預期的後果。

4. 建立單位資安聯繫管道，時刻掌握資安情資

單位應建立資安專責聯繫管道，負責接收與回報資安情資與資安事件，平時多關注相關資安新聞、漏洞發布資訊等資安情資(如加入 TWCERT/CC 臉書粉絲專頁及訂閱 TWCERT/CC 電子報等)，適時參與資安研討會以了解最新的資安威脅趨勢與防護技術，並將所獲情資對內部員工進行宣導，以培養員工之資安意識。當內部發生資安事件時，協助員工進行事件排除，並可依事件影響等級對外通報及尋求協助(如向 TWCERT/CC 通報)，以求事件之快速排除。

二、 法規的限制

1. TWCERT/CC 針對通報的問題之驗證無法源依據

由於 CERT 通常屬民間之非營利組織，因法規關係，除通報網頁置換

或釣魚網頁等可直接檢視外之案件外，部分接獲之通報案件所述之通報問題無法即時或有授權可驗證情資是否正確，難以確認通報情資正確性，若不經求證之通報而造成誤報，將造成受通報單位之不便，更使通報單位之可信度受質疑。

例如：有大量屬於台灣用戶的電子郵件帳號及密碼遭到公布在其他國家之網站上，並無法得知被公布之原因。當 TWCERT/CC 接獲該情資時，若嘗試驗證其帳號密碼之正確性時，可能遭質疑有入侵嫌疑。

2. 系統代管或開發商處理資安事件態度消極

系統開發商或託管商認為其開發的產品遭通報有資安疑慮時，為了避免事件擴大影響其公司開發系統的品質遭質疑，卻僅關閉或移除問題資料，且不願意讓其客戶知道此事件。

例如：資訊系統開發商或託管商表達不應該將產品問題通報其客戶，應直接通報至該業者。

3. 受害單位認為即使有影響其他人也無所謂

當企業或民眾接獲資安通報後，即使說明此通報可能造成的影響，仍不願意修補。

例如：企業或民眾購置的網路監視器遭公布於 Insecam 網站時，即使了解若未修正相關設定，可能遭駭客植入惡意程式，成為殭屍網路的一員攻擊其他設備，但是企業或民眾認為不是攻擊自己，因此不認為有影響。

針對法規上的限制而造成資安通報與協處程序的挑戰，TWCERT/CC 建議之改善對應策略如下：

1. 提供通報問題驗證方式

受限於資安情資驗證時，須經當事者同意，因此，通報單位如能協助整理相關驗證方式之資訊，由受通報單位自行確認，便無觸法疑慮。

2. 公布通過資安檢測的合格開發商資訊

當企業或民眾需要委託系統開發商建置其系統或網站時，可透過公開資訊網站查詢經過資安檢測認證合格的開發商，形成良性競爭關係。

3. 強化資安政策及法令規範

應該修訂法律規範，若確實有資安疑慮時，應該配合修正，以避免成為加害者。

綜上所述，TWCERT/CC 進行通報業務時，面對之挑戰不外乎企業或民眾資安意識不足，導致資安問題重視程度低落，若能將基本資安觀念推廣達到全民化，如此不論企業或個人都將有效減少資安事件發生，以建立良好之資安環境。

References

[1] NetAdmin, "已知漏洞才是遭駭大宗　資安莫再捨薪輿而逐秋毫", Retrieved Jan. 15, 2018 from the World Wide Web: http://www.netadmin.com.tw/article_content.aspx?sn=1801030010

[2] iThome, Jan. 11, 2018, "你的 Windows 更新了嗎？當心防毒軟體和修補程式不相容導致無法更新", Retrieved Jan. 15, 2018 from the World Wide Web: https://www.ithome.com.tw/news/120464

[3] Microsoft, May 14, 2017, "為協助抵禦大規模惡意勒索病毒的侵襲，請用戶立即安裝微軟於三月釋出的安全性更新 MS17-010", Retrieved Jan. 15, 2018 from the World Wide Web: https://news.microsoft.com/zh-tw/windowsdefender/#sm.0000535813159xdpuvym8a1p5ik3g

[4] 許登傑, "淺談安全軟體發展", Retrieved Jan. 15, 2018 from the World Wide Web: http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=2115

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