用攻擊思維搶先防禦　漏洞獎勵計畫廣邀高手賺獎金

設備商成立駭客團隊 保障用戶避免資安風險

文◎洪羿溎

為了遏止層出不窮的軟體漏洞導致企業損失，近年來全球興起漏洞獎勵計畫（Bug Bounty），企業開始效法國際指標型資訊科技大廠Google、Facebook、Microsoft等，吸引頂尖駭客共襄盛舉。NAS製造商群暉科技（Synology）亦發起安全性弱點獎金計畫（Security Bug Bounty Program），並且成立產品安全應變小組（PSIRT），延攬國內資安界技術高手專職負責漏洞分析與重現，進而協同研發單位及時修補與發布更新，以保障用戶安全。

現任群暉科技產品安全事件應變小組的安全分析師鄭達群，交通大學資工研究所畢業後即加入該小組，三年期間已參與回應許多重大資安事件，例如Heartbleed、SambaCry、破解Wi-Fi WPA2的KRACKs等漏洞。之所以擁有一身駭客攻防戰的技能，來自於大學期間選修程式碼安全課程，教授採以CTF（搶旗攻防賽）的方式來進行，儘管難度頗高，鄭達群卻反而感到有趣，甚至進入到研究所後，開始進一步研究CTF所有曾經出現過的考題，思考解答的方法，並以參加駭客最高聖殿DEF CON CTF攻防賽為目標，一頭鑽入研究學習與訓練。

2014年，鄭達群就讀碩士一年級時，所參加的台灣HITCON駭客戰隊終於打入總決賽，由趨勢科技贊助前往美國拉斯維加斯與國際頂尖駭客選手一較高下，取得第二名的優異成績，新聞媒體紛紛以「台灣之光」大篇幅報導，不僅打響HITCON駭客戰隊名號，同時也讓更多人開始關注資安議題。

制定SOP盡速排除問題 降低用戶損害

在共同創立交大Bamboofox社團的學長引薦下，鄭達群自研究所畢業後隨即加入群暉科技。他也不諱言，儘管擁有一身駭客攻防戰的技能，也難以立即掌握產品技術架構，因此初期約有半年的時間是從事研發工作，藉此熟悉產品開發流程，待熟悉後才開始承接產品安全應變工作。

接手安全性弱點獎金計畫之後，他開始積極制定標準作業流程，讓產品安全應變小組有所依循來處理通報。實作上大致分為四個階段，包含發現問題、評估安全等級、修復與揭露。鄭達群進一步說明，發現問題方面主要是針對非營利組織MITRE最新發布的CVE漏洞編號或Boynty通報，必須深入分析後才得以評估問題的安全等級階段。

「我們在產品架構中採用不少開源碼軟體，所以必須掌握不同管道的第一手資訊。主要是以郵件討論串為主，同時也關注國際廠商發布的資安情報，例如Red Hat就勢必參考，主因在於Linux版本較為接近，因此一旦Red Hat有潛在漏洞被揭露，產品線受影響的機率也很高。另一個原因是Red Hat畢竟是國際大廠，對於漏洞的分析與處理細節會提出完整報告，可直接參考提高應變效率。」

進入到評估安全等級階段，重點則在於確認問題是否會發生，有可能產品線剛好沒有採用隱含漏洞的功能或系統核心版本。萬一經過分析後確認，首先會透過郵件通知負責研發的承辦人，以釐清受影響的功能性與涉及的產品線。

取得研發單位回饋之後，隨即可進入修補問題。最簡單的狀況是系統核心版本升級即可解決，這也是每次推出更新修補程式時較多採用的作法；但若是緊急問題，例如檔案分享系統出現漏洞，則必須以最快的時間準備新版本供用戶即時升級更新，以免遭受攻擊威脅。

最後是安全性諮詢建議，根據已發現的漏洞，評估受影響等級與範圍較為嚴重，需要公告周知時，則會撰寫該漏洞的完整分析報告，說明危害程度、影響的功能性、涉及的韌體版本與設備型號，最後是提供緩解方式，可能有些漏洞根本毋須安裝更新程式，只要調整或關閉特定功能即可免於遭受攻擊。

掌握最新漏洞資訊 協同研發修補更新

談到CTF競賽，其實主要運用真實世界的漏洞，經過簡化設計後成為比賽題目，只是CTF競賽通常時間不長，最多為48小時，即使在真實世界尋找漏洞並沒有時間限制，也無法彼此參照，兩者之間差異頗大。鄭達群舉例，在CTF競賽遇到購物車網站環境的考題，若僅發現訂購功能，即可推論題目應屬於購物流程類型。但是，真實世界評估產品研發漏洞並非如此，可能只能觀察到現象，執行買賣、儲值等行為，往往難以明確得知漏洞可能發生的環節，必須在全部功能都正常運行的狀況下，先找到潛在風險性。

▲在本土駭客圈相當活耀的鄭達群提醒，過去大眾對於駭客的負面觀感較重，直到近幾年方逐漸扭轉，也才得以公開談論與交流學習經驗，但學習駭客攻擊的技術人員仍須謹守分際，否則一旦行為出現偏差將會害人誤己。

不過職責上，產品安全應變小組的任務並非在產品推出後仍持續不斷地尋找漏洞，主要業務範圍是處理已經發現的漏洞，快速地提出修補更新；或者是透過安全性弱點獎金計畫，由外部的駭客組織通報的漏洞，著手進行分析，設法重現漏洞，以確認影響程度。

所謂重現漏洞意即類似於競賽解題，利用漏洞來設計攻擊程式，拿到Flag即可得分。除了在DEF CON有攻防的賽制以外，其他的CTF不大會考慮漏洞修補的環節，只要知道怎麼利用來攻擊即可。然而維護產品安全性的工作，除了分析重現漏洞，更要考慮的是修復方法，避免客戶端設備遭受攻擊。

「當然，正式修補還是必須得交由研發部門來執行，我們的職責是能夠重現問題讓研發單位理解，彼此先取得共識後，討論修補方式是否影響功能性，以及有效性。畢竟修復產品漏洞並非僅只是專注於解決資安問題，必須得在不影響程式碼正常運行下進行，只有研發團隊才能完整掌握與判斷。」

研發階段減少漏洞 數量才是最佳防護

本土許多優秀的資安人才，不是進入資安原廠，就是自行創業，鄭達群的選擇卻是系統廠商，主因在於他認為資安領域專業度較高，即使是高科技製造廠商也必須設立專職資安人員，而非把責任全交給研發人員，否則恐難免會有不足之處。

「事實上，早期大家對於駭客的印象就是搞破壞，利用漏洞隨意入侵其他人設備，現在有個工作可以把我在求學時代學習到的知識，應用在工作上，是一件很令人開心的事。多數人的際遇反而是無法學以致用。」

現階段若要期待研發人員也懂得駭客攻擊手法，在程式開發階段就予以避免，恐怕過於理想化。但是以長期來看，程式開發安全的資安教育確實有其必要性，強化研發人員對於攻擊手法的知識，在開發階段直接設計迴避方法，才可從根本上解決問題，因此除了處理已知的漏洞，同時也協助在產品開發初期時，提出設計想法與評估程式邏輯是否具有潛在資安風險。「減少漏洞的數量，正是產品安全最根本的防護方式。」他強調。網管人