DELL Technologies

從勒索軟體攻擊中學習到的教訓

巴塞隆納自治大學案例分享

Gonçal Badenes
巴塞隆納自治大學資訊長
採訪經過重點整理和編輯，方便讀者掌握重點。

對更新網路安全性的迅速行動、透明度和重申承諾，勾勒出大學因應勒索軟體攻擊的方式。

Dell Technologies 網路安全性行銷部的 Sameer Shah 與大學資訊長 Gonçal Badenes 談論此一事件。

Shah：我們一直在談論幫助組織逐步提高網路安全性成熟度的需求。以前你們都遭受過網路攻擊。在我們深入探討攻擊的更多細節之前，您能告訴我們一些關於大學及其 IT 環境的資訊嗎？

Badenes：巴塞隆納自治大學是西班牙的頂尖大學之一。IT 監督大學運作所需的所有服務。

就在攻擊發生之前，我們有一個改善網路安全性狀態的完整計畫。我們已經部署了多因素驗證 (MFA)，但並未涵蓋所有服務和使用者。學生和所有 IT 員工都已經擁有 MFA，但僅限於 Microsoft 365 平台。其他服務未受到保護。我們在之後發現，缺乏通用 MFA 的影響重大。

攻擊是什麼時候發生的？是什麼樣的攻擊？

這是一次在連假發生的勒索軟體攻擊，與其他常見案例如出一轍。清晨四點左右，我接到團隊的電話，說有多項服務像骨牌效應一樣接連中斷。他們發出了警報，我們便立即召集預先為這類案例規劃的應變小組。

您怎麼知道這是勒索軟體攻擊？有贖金說明檔案嗎？

受影響的系統上有贖金說明檔案。而且他們還執行指令檔來加密週末期間有在線上的電腦，發動了小型攻擊。這樣做的影響是有限的，主要目的可能是確保員工和學生發現攻擊，而不只是讓 IT 團隊發現。

在那段期間內，您的組織是否曾經考慮支付贖金？

否。

原因為何？

從道德的角度來看，我們做不到。幸好我們有備份，其中兩個副本位於校園內的兩個不同的資料中心，第三個副本則位於組織邊緣外的磁帶上。

我想確認一下，這些備份不是資料存放庫，對吧？

對，當下還不是，我們沒有存放庫。這是藍圖上的未來優先事項。但存放庫接著 [在攻擊之後] 當然成為優先事項。

在這些情況下，溝通可能至關重要。聽起來，您透過清楚、透明的溝通，包括與媒體的溝通，及時阻止了攻擊？

對，從第一天起。我們必須完全透明，並盡可能公開，解釋發生了什麼事。我們想要確保其他人可以作好準備，並從我們的經驗中學習。我猜是某些媒體實際上閱讀了贖金說明檔案並聯絡了攻擊者，因為我們從未這樣做過。攻擊者組織自稱為 PISA (「Protect Your System, Amigo」，意為「朋友，保護您的系統」) 集團。

很多時候，組織更喜歡保密，以避免暴露他們的弱點或補救策略。這是疑慮嗎？

這些都是非常合理的疑慮。但我很確定，我們都知道本身有弱點。當我們試圖保護自己的家時，我們知道就算我們買了最好的門，如果強盜真的想要動手，他們也會想辦法破門或找到其他方法進入。這是完全相同的道理。

我們受到攻擊而且有漏洞，這個事實沒什麼好不敢承認的。事實上，我們要與人們分享的一個重點，就是我們有一個非常明確的保護藍圖，但仍然受到攻擊。即使我們有一些非常好的保護，我們仍然有可能會受到攻擊的漏洞。透過實施其他步驟，您可以處於更有利的形勢。

請告訴我們，您立即採取了哪些行動以開始解決問題。

我們關閉了所有系統的網路。我們聯絡了警方和地區機構進行資料保護，這是我們必須做的法定事項。然後我們立即成立了兩個團隊：鑑識和復原。我們致電 Dell，然後對方立即將這個事件呈報為第一優先，而且我們獲得一個非常了不起的團隊，他們馬不停蹄地處理這個事件。他們設法完全還原了第二個 Data Domain 上的所有資料。

所以鑑識是在還原程序期間開始的？

對於某些還原程序，我們不得不稍等片刻。這就是為什麼我說首先開始鑑識。因為需要瞭解發生了什麼事，所以隔離了一切。我們必須安排另一個系統，這樣我們才能開始還原一切。我們決定，就算我們會花更長的時間，所有上線的系統也都必須達到最佳安全標準。

「我認為最重要的考慮事項，就是我們遲早都有可能會受到網路攻擊，因此我們需要制定詳細的緩解和還原計畫。」

您提到僅在 Microsoft 365 上實施 MFA，而這是導致攻擊者得以發動攻擊的部分原因。那麼，現在是否全面實施 MFA？

攻擊的手法是竊取所在團隊已在 Microsoft 上使用 MFA 之使用者的登入資料。但是，當攻擊者嘗試存取電子郵件並發現由於 MFA 而無法得逞時，他們就繼續搜尋。然後，他們發現我們有一個未受 MFA 保護的 VPN。一旦他們透過 VPN 取得存取權，就可以開始調查網路。

在像我們這樣非常大的網路中，他們發現了一個有漏洞的系統，並開始橫向移動。所以此時，在我們開始還原系統後，我們決定所有項目都要受到 MFA 保護才能上線。

如果要給同行一個重要建議或忠告，以避免勒索軟體攻擊，您想說什麼？

給出一個忠告非常困難，但我認為最重要的考慮事項，就是我們遲早都有可能會受到網路攻擊，因此我們需要制定詳細的緩解和還原計畫。

舉例來說，擁有鑑識和復原方面關鍵合作夥伴的聯絡人、擁有詳細且有優先順序的服務圖與復原的時間表，以及與關鍵業務部門 (包括通訊 [內部和外部]) 制定一致的策略，非常重要。當然，讓使用者保持警惕並接受有關攻擊者所用技術的訓練，也很重要。

您覺得，大學網路安全性能力的加強是否讓您更有信心繼續履行使命以及您正在做的所有偉大工作？

當然適合。在攻擊事件之前，其中一種常見觀點，就是任何保護系統的新措施都會受到很多質疑，以及我們是否真的需要這些措施的疑慮。事實上，保護絕對是必要的措施，否則會把整個企業置於危險之中。當然，有些人仍然認為這些措施阻礙了他們的工作。但大多數人認為，系統得到了更好的保護。

感謝您。您的坦率和透明資訊，對每個致力於提高網路安全性成熟度的人都有幫助。