案例分享–某企業AD上百組帳號大量登入失敗導致鎖定事件

- 11月 22, 2022

雲智維科技
Cloud Intelligent Operation,CIO

某企業AD上百組帳號大量登入失敗導致鎖定事件

一、案例故事

某企業客戶於某日下午發生Exchange遭受外部惡意主機大量進行暴力破解攻擊，導致企業內部環境AD伺服器短時間內被鎖定一百多筆帳號事件，而該企業也有在Exchange的WebMail上啟用雙因子認證，還是在短時間內遭受大量暴力破解攻擊，尋求雲智維科技團隊協助。

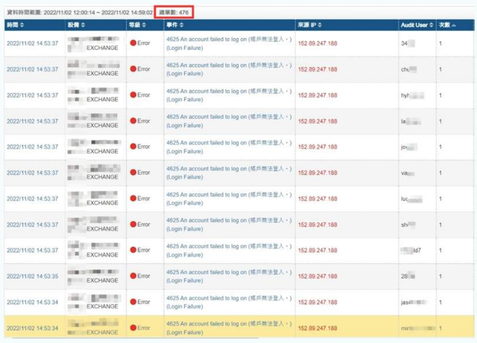
二、解決方案

使用「雲智維資訊顧問代管代維方案」，透過收集客戶單位中各種網路設備syslog、資安設備syslog、Flow及SNMP，從各式數據搭配AI即時分析，從中查找出重要的關鍵數據，找出客戶內部環境網路、資安問題所在。

該企業使用「雲智維資訊顧問代管代維方案」，可從Exchange稽核紀錄中查找登入/登出稽核紀錄，並發現到有大量帳號登入失敗、猜測的紀錄。

點擊查詢詳細資訊，發現有外部IP使用多個帳號大量嘗試登入、猜測紀錄。

藉由統計功能，發現到該IP總共使用了476組帳號進行嘗試



再藉由客戶所導入的Exchange IIS紀錄中，有發現到外部嘗有大量連線到Exchange的「/Autodiscover/Autodiscover.xml」此路徑下

查閱相關事件，可得知該路徑「/Autodiscover/Autodiscover.xml」服務，能被有心人士發動Exchange Server觸發對外Autodiscover.* 網域名稱查詢導致帳密遭竊聽外洩。

建議措施:

1.啟動聯防封鎖惡意來源攻擊者。

2.封鎖企業對Autodiscover.* 網域名稱查詢，以避免內部所有帳號密碼外洩的風險。

漏洞紀錄：https://www.ithome.com.tw/news/146842

三、結論

該企業導入使用「雲智維資訊顧問代管代維方案」，有效解決了企業面臨發生大量暴力破解攻擊時，導致AD網域帳號被鎖定事件時，能夠快速收斂問題點所在，給予相關建議並改善，讓企業網路維運與資安安全等級更加提升。

案例分享 AD事件 Exchange攻擊

位置： 雲智維科技