ATM入侵事件的分析與建議

❖從本次ATM封閉系統被入侵事件，目前管理上的漏洞重點條列如下：

一. 未受管理的特權帳號：為了管理方便，所有系統、派送軟體都使用同一個密碼，造成無法勾稽，也無法作權限控管。只要這個密碼被盜用，任何的防護機制都失效，而且更可以作到植入惡意程式、控制硬體的行為。

二. 手動白名單無效：多品牌，多作業系統，從NT, XP, 2000, 2012, WIN7，多版本，不可能有統一的白名單。 手動建立不但耗時耗力，重要的是不可能準確。

三. 異常行為未即時警示：只作到事後的勾稽，入侵過程有非常多的動作與準備，這類的異常動作沒有即時警示機制，造成無法即時阻擋。

❖建議解決方案：

一. 應建立類似特權帳號OTP機制，回收ATM端末的特權密碼，並建立更簡易的電子化系統，提供線上申請、自動變更密碼等機制，並必須可以跟ATM派送系統作整合，在ATM派送系統時可提供密碼。

二. 手動建立白名單已証明不可行，只能透過自動學習，在測試環境上自動學習每一個系統、版本的允許執行程式白名單，在軟體派送時一併把自動學習的白名單派到各端末。

三. 建立異常行為即時警示：駭客的連線一般都包括許多的不正常行為，如能先期發出警示，就能作到主動的防護。包括用戶不正常時段的登入連線、用戶連線次數大量增加、機器不正常時段連線、不正常IP位址連線、機器連線次數大量增加、未授權登入(帳號被盜用) 、未納管後門帳號、異常登入來源機器、用戶異常登入、異常登入目標機器。依本次ATM入侵行為模式分析，這些異常行為確實能有效即時警示管理人員進行了解與處理。

Cyberview 力悅資訊
取得更多訊息，請聯絡：02-25071601
E-mail: sales@cyberview.com.tw