應對勒索軟體，備份並不足夠

備份固然很好，但是為何還不足以應對勒索軟體？

“勒索軟體”最近發生機率似乎大大的提高，報紙、雜誌、訊息安全報告以及其他所有警示人們訊息安全威脅的地方都能看到它的身影。我們也許會將 2016 年稱為”勒索軟體年”，但和 2017 年相比卻不值一提。在相對平靜的 2018 至 2021 年之後，2022 年一直都是資訊安全的新聞頭條。

很多勒索軟體的文章，幾乎所有文章都提出了以下三條建議：

1. 使用可靠的端點安全保護措施。
2. 避免從可疑網站上下載可疑文件，或打開可疑人員發來郵件中的可疑附件，並對員工進行相關主題的培訓。
3. 定期備份重要資料。

然而，我不時聽到這樣的反對意見：

保護程式和提升員工意識是很好的防護措施，但是，當我們可以定期備份所有內容時，為什麼還要大費心思加強防護和進行員工培訓呢？如果我們被勒索軟體攻擊，我們只需要恢復所有文件，難道不是嗎？那麼接下來讓我向你解釋，為什麼備份不能解決所有的問題。

備份必須可完整還原

備份當然是必要的，但你是否嘗試過利用備份還原公司的資訊系統呢？這實際上可能比聽起來複雜得多，並且你擁有的資訊系統越多，還原備份就越困難。經驗豐富的 IT 專家可能都遇到過備份無法完全還原所有內容的情況，或者還原結果不完全如意。毫無疑問，整個流程也沒有他們期望的那麼快，而且有時備份根本不起作用。

曾經使用過備份工具的人都知道，他們必須定期檢查備份的完整性，在測試環境中測試伺服器的還原機制，並且總體上確保在必要時進行還原的時間不會花費過長時間。如果你從未嘗試過還原備份的人，那麼你不應該小看這項任務，因為你無法保證在危急情況下備份可以立即發揮作用。

過分依賴備份還可能遇到另一個問題：如果備份伺服器位於網路內部，那麼勒索軟體會將它與所有其他電腦一起加密，這意味著備份還原計劃完全不起到任何作用。

最起碼應對措施：通過設置網路，合理規劃備份並定期測試還原備份，或者備份具備不可變動性的機制，從而最大化快速回滾系統的可能性。

恢復備份意味著當機，而無法還原的代價很大

對於有各種設備和基礎架構的大公司，快速恢復幾乎是不可能的任務。即便備份功能完美運行而且你也傾盡全力還原所有內容，整個流程仍然需要花費一定的時間。

在這幾週時間裡（是的，可能是幾周而不是幾天），公司的業務將受到極大影響。有人估計當機造成的損失會少於支付給勒索者的贖金（我們強烈建議不要這樣做）。無論是還原備份還是支付贖金，遭受勒索軟體攻擊後的無法恢復是不可避免的。即使網路犯罪分子良心發現為你提供解密程序，解密並重新運行所有系統也需要花費時間。在現實生活中，別指望網路不法分子會如此客氣，而且解密工具也不一定能如預期中那樣起作用。

最起碼的應對措施：要想避免勒索軟體導致的當機，你應該盡力避免感染勒索病毒。（但如何不被感染？答案是做好防護措施以及員工意識培訓！）

現代勒索軟體不僅僅是加密那麼簡單

勒索軟體犯罪團體過去主要以終端客戶為目標，並索要價值約 300 美元的加密貨幣作為解密贖金。然而，他們現在意識到了攻擊企業的收益更大，企業會（至少更可能）支付巨額贖金。一些網路不法分子為了利益無所顧忌地攻擊醫療組織。許多醫院受到了攻擊，包括最近一家負責新冠病毒疫苗供應鏈的公司。

現如今，勒索軟體不僅僅只有加密那麼簡單，它潛伏在網路中並竊取發現的所有資訊。隨後，犯罪團體會分析數據並以加密或（和）洩漏數據來威脅企業。勒索軟體的訊息可能聲稱，拒絕支付將導致客戶個人數據或公司商業機密被公開。即便這些數據可能並非十分關鍵，這也會對公司的聲譽造成傷害，甚至可能是永久性的。同時，這樣的數據洩露可能會導致公司與《個資保護法條例》的監管機構等進行一些說明。如果入侵者執意洩漏公司機密或用戶個人數據，備份並不會起到任何作用。此外，如果你將備份儲存在雲服務，內部人員相對來說會比較容易訪問這些數據，理論上他們有可能已被攻擊者鎖定提供入侵者所需要的訊息。

最起碼的應對措施：備份十分必要，但是僅僅依靠備份無法保護你的企業免受勒索軟體的攻擊。

防範勒索軟體的三個要點

再次提醒，因為沒有專門針對勒索軟體的工具，我們仍然建議備份，但必須通過正確的方式進行備份，並且需要一定的投入以及多次備份還原演練。所謂的投入包括了解備份的具體細節：備份的頻率及其存儲位置及備份不可變動性機制。所有負責相關事項的員工必須知道具體如何快速地重新啟動對系統的操作。保護措施也必不可少，不僅需要應急響應，還需要主動保護，避免安全威脅在網路中擁有立足之地。同樣重要的是，要對員工進行網路安全基本常識的訓練，並定期檢測他們所學的知識。

簡而言之，企業的網路安全歸結為三個詞：備份、保護和意識。這三點都需要落實到位，然後你便可以自信地宣布你正在使用最佳的抵禦勒索軟體安全策略。

建議解決方案

高防護力的端點安全保護

專為中小型企業開發的 Kaspersky Endpoint Security Cloud(KESC)雲端管理防護平台，讓您可以從任何地方遠程管理多個端點、設備和伺服器的安全性。

多層次端點防護平台，搭載採用 HuMachine Intelligence 的新世代網路安全技術，可以透過機器學習引擎、可疑行為偵測、控制、資料防護等靈活的自動化防護，防止無檔案攻擊和勒索軟體等最先進的已知和未知威脅。

可以有效進行未知事件模擬自動 阻擋，來對抗複雜威脅和 APT 等級的攻擊，而且可以和 Kaspersky Endpoint Security for Business 緊密整合。

可在面臨複雜和進階威脅時，透過提供進階偵測、簡化的調查與自動回應，來協助分析建立真正的縱深防禦。

省時完整還原防加密備份機制

NAKIVO Backup & Replication.

提供虛擬、實體、雲端和 SaaS 的勒索軟體保護方案

無代理、應用程式感知備份
執行無代理，可識別應用程式的增量備份

虛擬機快速啟動與精細還原
快速啟動完整的虛擬機或從虛擬機備份來還原檔案或是應用程式物件

備份到多重目的端
本地位置、雲端空間 (Amazon S3, Wasabi, Azure), 異地端、磁帶

勒索軟體防護備份(不可變動性)
可使用本地儲存區或Amazon S3 Object Lock來達成不可變動性儲存資料

自動化備份
將您的資料保護作業設定為自動執行

性能優化
縮小備份、 LAN-free 資料傳輸、全域式重複資料刪除等等

備份/副本驗證
可立即確認備份/副本是正確的而且可被還原

災難還原
自定義災難還原SOP和不中斷生產環境的自動化測試

安全意識培訓規劃

Proofpoint Security Awareness Training

30 個以上訓練模組內容/35 種以上語系支援(含繁體中文)/社交工程演練

https://www.htservice.com.tw/

解決方案：https://www.htservice.com.tw/?page_id=167
委外維運服務：https://www.htservice.com.tw/?page_id=592
資安分享：https://www.htservice.com.tw/?page_id=173

禾滔科技有限公司 HT Service
電話：02-7709-7779
地址：台北市內湖區瑞光路 513 巷 26 號 7 樓之 2
咨詢信箱：msp@htservice.com.tw

卡巴斯基白金級
銷售及技術服務認證