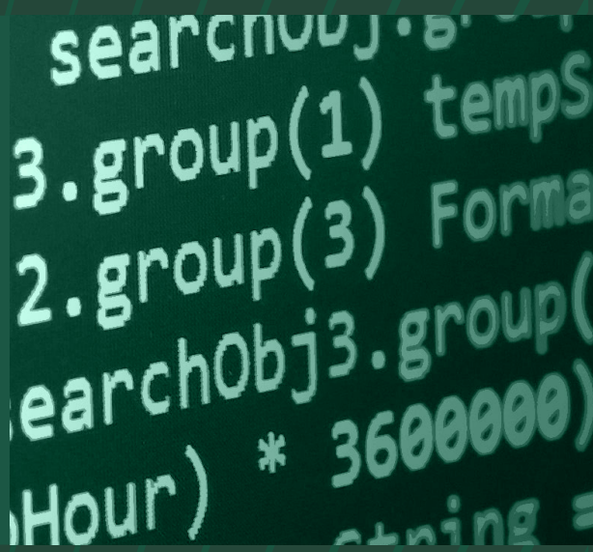
DELL Technologies

5 如何承受勒索軟體攻擊的建議



1 維持全面的事件應變計畫

- 著重將攻擊的影響降至最低
- 經常練習、測試和更新
- 提前準備好事件應變團隊
- 將網路保險視為整體復原能力策略的一部分
- 納入與執法機關合作的計畫

2 制定明確的通訊策略

- 提前建立通訊範本
- 確保組織內部及時和明確的溝通
- 做好對外溝通的準備 (若適用)
- 遵守適用的通知法規

3 確保強大的資料保護

- 在隔離、不可變、實體隔離的資料存放庫中，保護關鍵資料
- 依服務/基礎結構排定復原的優先順序
- 實踐復原能力
- 將無塵室等功能與回復時間目標配對
- 確保可復原資料的完整性

4 不要假設可以立即恢復正常

- 支付贖金應是最後手段
- 付款前確保符合法律和法規要求
- 即使支付贖金，也無法保證駭客會歸還您的資料

5 強調訓練和教育

- 進行攻擊模擬
- 監控和測試員工的網路安全衛生做法
- 使用網路釣魚測試和電子郵件安全訓練等工具

這不再是「如果」，而是「何時」的問題。

儘管企業採取了最好的防禦措施，仍必須假設攻擊不可避免，並做好規劃。針對這個議題，網路安全及法規遵循實務全球總監 Jim Shook、網路安全解決方案與策略性合作關係首席顧問 Steven Granat，以及 Dell 資料保護產品行銷資深顧問 Brian White 等 Dell 主題專家齊聚一堂，討論在災害發生時應該怎麼做。

> 「你必須找到合適的人加入、進行演習並模擬行動，這樣當攻擊發生時，每個人就可以立刻知道要做什麼。」
>
> ***Steven Granat**，首席顧問*
> *Dell Technologies 網路安全解決方案與策略性合作關係*

維持全面的事件應變計畫

當攻擊發生時，所有關鍵利益關係人 (幾乎包括組織中的所有人，以及供應商等第三方) 都必須知道該怎麼做。Shook 建議，書面事件應變計畫應列出明確的行動順序。全面的計畫將涉及從立即行動到復原的技術、流程和通訊步驟。務必也保留紙本文件，因為數位通訊模式可能無法運作。Granat 表示：「就字面意義來說，你需要一個可以直接從架上拿下來使用的計畫。」

制定明確的通訊策略

大多數組織將必須與關鍵利益關係人溝通，而且在許多情況下，必須遵守法規要求。為內部和外部通訊建立不同的範本，其中包含應通知哪些人員、通知順序和時間點的系統化指示。也要規劃電話和電子郵件系統停擺時的做法。

實行完善的資料保護策略

承受勒索軟體攻擊的一個關鍵目標，是回復資料並盡可能無痛地還原，同時避免支付贖金。強大的資料保護策略是實現這些目標的關鍵要素，但需要納入技術和流程。Shook 建議：「使用不可變的資料和網路存放庫來儲存足夠的資料，讓您可以信任或至少作為驗證點，進而能夠還原系統。」第一步是確保資料受到保護；此外，您還必須擁有適當的人員和流程來還原資料。第三方專家可以提供協助，但應該在規劃階段就加入。

即使您支付贖金，也不要假設可以立即恢復正常

支付贖金只應被視為最後手段，並不能保證一切會立即恢復正常。請記住，您正在與犯罪分子談判，即使您已確實取得解碼金鑰，也需要為新還原的資料制定策略。首先，您必須測試解密的資料，並有條不紊地重建所有系統。在攻擊發生之前，反覆地仔細關注假設情境，對於實現復原能力大有裨益。Granat 表示：「瞭解您技術基礎結構中的不同應用程式和相依性，對於高效還原至穩定狀態，至關重要。『我是否有可行的復原來源和可復原的目標？』、『我是否有不會洩露的資料？』，這些都是需要考慮的重要因素。」

在復原階段，您還需要確保攻擊者實際上已離開您的系統。Shook 表示：「比方說，你必須確保房子已經完全滅火，並找出一開始是什麼引發了這場火災，因為如果沒有這兩個關鍵資訊，你就會讓自己在未來容易受到攻擊。」

訓練和練習至關重要

網路韌性很重要的一個部分在於全方位訓練，從確保員工貫徹嚴謹的網路安全衛生，到復原計畫的例行練習。Shook 表示：「你必須找到合適的人加入、進行演習並模擬行動，這樣當攻擊發生時，每個人就可以立刻知道要做什麼。」

在現今的威脅態勢下，可能無法避免勒索軟體攻擊發生，但透過規劃和執行，您可以將攻擊對營運、財務和聲譽的影響降至最低。目標是盡可能快速無痛地恢復正常。

造訪 **dell.com/cybersecuritymonth**，瞭解如何解決當今一些主要的網路安全挑戰

DELL Technologies