安全遠端存取

風險何在？

#1

不安全的遠端存取，成為對實體商家發動攻擊的切入點

（遠端存取技術最佳實務）

不安全的遠端存取，是企業資料外洩的一大成因。

銷售點 (POS) 廠商經常是自其辦公室而非在營業地點對商家付款系統提供支援或進行故障排除。其作法是利用網際網路，以及稱為「遠端存取」類的軟體產品。這類產品許多始終保持開啟或隨時可用，換言之，廠商隨時能從遠端存取您的系統。

這類廠商有許多是以一般為人知的密碼進行遠端存取，導致駭客也能輕而易舉地存取您的系統。不肖之徒會從網際網路搜尋遠端存取系統有所弱點的企業，一旦得其門而入，便能使用惡意軟體盜取寶貴的支付卡資料。

遠端存取最佳實務

為將資料外洩的風險降至最低，對於廠商如何以及何時能存取系統的事宜，您務必參與管理。應限定必要時方能進行遠端存取！

對遠端存取的使用設限

詢問廠商如何在具體請求時啟用遠端存取，以及如何在不需要時加以停用。

要求採行多重要素驗證

若您必須允許遠端存取，請要求廠商採行多重要素驗證以支援您的企業。

要求使用唯一憑證

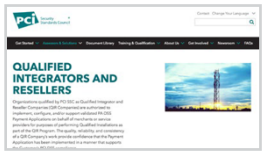
若您必須允許遠端存取，請確定廠商使用對您的企業為唯一的遠端存取憑證，不可用於其他客戶。

多重要素驗證能除了使用者名稱與密碼之外還多要求滿足一項要素（例如智慧卡或硬體鎖），為您的企業接受遠端存取提供保障。硬體鎖是一種便利的裝置，連接到電腦可允許存取無線通訊、軟體功能等。

資源

請瀏覽 pcissc.org/Merchants 取得更多資源

該以哪些 PCI SSC 問題詢問您的廠商資源能協助企業自協力廠商取得您所需要的資訊。



PCI Qualified Integrators and Resellers (QIR) 清單 是企業能用以尋找付款系統安裝者的資源，其受過支付卡產業安全標準委員會 (PCI Security Standards Council) 就安全遠端存取和其他付款資料安全要項所提供的培訓。

安全付款指南可為企業提供防範付款資料遭竊的安全基本知識。

請看這段動畫短片，了解企業可以如何藉由僅於必要時允許遠端存取，並採取多重要素驗證，將資料外洩的可能性降到最低。

PCI Security Standards Council