NTT Security

迎擊網絡威脅:
金融機構應對網絡安全威脅的最佳實踐

針對金融機構的網絡威脅正不斷增加

2014年, 本港的互聯網威脅在亞太區的排名58位

資料來源:成報

金融機構面對的網絡攻擊是其他行業的 **3 倍**

資料來源:香港銀行學會

平均每年網絡罪行帶來的損失高達 **5千9百73萬港元**

資料來源:香港銀行學會

自2014年起, 金融界檢測到的惡意軟件有高達 **140%**的增長。

資料來源: *NTT Group 2016*全球威脅情報報告

超過**12%**的漏洞問題已經潛在超過5年, 而當中5%更潛在超過10年

資料來源: *NTT Group 2016*全球威脅情報報告

平均只有**23%**的機構能有效應對網絡保安事故

多達**77%**的機構沒有能力應對關鍵事故, 而且往往在事故發生後才購買事件響應服務

資料來源: *NTT Group 2016*全球威脅情報報告

「網絡防衛計劃」

- **網絡防衛評估框架(C-RAF)**是由香港金融管理局和銀行界合作推出的「網絡防衛計劃」的其中一個支柱。
  - 網絡防衛評估框架是一套風險為本的框架, 讓銀行**評估本身的風險狀況**和需要採取的防禦措施及保安水平, 進一步**提升銀行體系應對網絡風險的能力**。
- 評估框架包含三個部分:

自身網絡風險評估

- 評估金融機構自身的網絡風險狀況
- 根據現時網絡風險狀況, 以「高」、「中」或「低」三個級別顯示其所屬的「自身風險程度」

網絡韌性成熟程度評估

- 此評估可用作衡量網絡風險程度, 及其網絡韌性的成熟程度
- 更可有助規劃並制定能加強網絡韌性的步驟

風險情報主導的網絡攻防模擬測試(iCAST)

- 測試採用模擬真實情境, 讓企業根據特定及最新的風險資訊, 來應對逼真的模擬網絡攻擊。
- 自身網絡風險程度被評為「中級」或「高級」的金融機構, 均要進行iCAST測試

應對C-RAF框架的關鍵步驟

安全操作服務
- 託管安全服務
- 定期滲透測試
- 事件響應服務
- 安全意識培訓

IT技術實施服務
- 確保客戶有效實施技術控制, 包括SIEM、UBA、IPS、NG-FW、DLP、NAC等
- 技術優化

IT架構規劃設計服務
- 幫助客戶設計IT技術解決方案
- 為客戶提供技術選項諮詢服務

網絡韌性評估服務
- 探查和確定當前的網絡風險
- 評估網絡控制對金管局C-RAF框架的有效性
- 優先化處理經識別的網絡安全風險差距
- 自身網絡風險程度評估
- 網絡韌性成熟程度評估
- iCAST模擬測試

策略性網絡安全諮詢服務
- 制定切實可行的網絡安全改進規劃

如你對NTT Security全球企業網絡風險評估方法有任何查詢, 請聯絡Marketing-APAC@nttsecurity.com

Copyright 2017 NTT Security