精誠資訊 2025/03/31 資安事件損害控制或復原作業現況報告

一、可能入侵管道與方式說明

1. 精誠資訊已向法務部調查局報案，並同時委託國際資安專業公司「趨勢科技股份有限公司」（下稱趨勢科技）進駐進行數位鑑識(IR)，調查可能影響範圍及程度。
2. 因數位鑑識分析需時，於調查數位鑑識分析過程如有明確發現，將會依以下方式主動告知：
   (1) 如有發現 IOC 情資(例如：中繼站與惡意程式)，立即提供政府與主管機關進行區域聯防。
   (2) 如有發現可能造成個別客戶損害風險，立即通知個別客戶與討論相對風險預防處理措施。

二、目前損害及復原作業說明

目前尚未有資料加密毀損與系統無法上線的實際損害，故尚無需復原作業。

三、損害控制機制(緊急應變)

1. 委請趨勢科技同時進行資安與網路架構檢視，評估可能的弱點後，進行相對強化修補調整。
2. 針對 AD、VPN 及核心系統等系統特權帳號修改密碼，同時強制整合多因認證機制(MFA) 以及擴大「特權帳號管理機制(PAM)」導入範疇，確保私密性。
3. 精誠內部 IT 單位針對核心服務系統皆有備份備援機制，每年均有定時進行備份還原演練，以確認資料的有效性與可用性。
4. 7x24 監控網路架構深度之資訊安全偵測設備(NDR)，從網路流量分析異常連線行為，如有發現，進行相對阻斷。
5. 擴大伺服器端及個人電腦安裝端點偵測與回應系統(EDR)，由趨勢科技 7x24 小時進行異常活動監控與回應處理(MDR)，降低惡意程式可能的損害衝擊影響。
6. 轉達與宣導同仁提高警覺：
   (1) 如有集團內部系統內容疑有異常（時間異常，金額異常，業務行為與內容異常），都與對方當事人進行「Double Check」真偽，並回報部門主管與資安單位。
   (2) 駭客可能寄送「電郵社交工程釣魚信件或者惡意附件」，已請同仁

於此段資安事件應處時間，提高警覺，針對寄件者為集團名義的疑似社交工程電郵內容，避免點選，同時通報資安同仁。

7. 為事前預防損害，採取以下措施：

(1) 針對與客戶間之郵件、檔案伺服器及專案管理系統，盤點與查詢有無機敏資訊（包括但不限於以帳號、密碼、Password、PW、個資、機敏、原始碼、弱掃報告等關鍵字盤查）。如有發現，評估衝擊性及是否啟動後續處理。

(2) 針對與客戶間之合約，檢視其中資安事故告知與通報規範，根據規定進行客戶通報，降低客戶可能的資安風險與損害。

(3) 針對與客戶間有資料交換/系統開發/系統串接者，評估衝擊性及是否啟動後續處理。

(4) 針對為客戶開發之源碼，使用「源碼檢測工具」以及「開源檢測工具」最新檢測規則進行安全檢測，如有漏洞弱點，規劃修補與更新為暫無漏洞版本（尤其是使用開源程式開發者）之計畫，提供客戶「最新源碼」。如果修補或更新有難度或者無法修補，將主動通報客戶可能的弱點與漏洞，與客戶協作透過客戶既有資安機制（例如：防火牆，入侵偵測系統，網站應用程式防火牆）進行補償措施與虛擬修補。

四、後續強化資安措施，加強集團資安精進與零信任措施如下：

1. 擴大佈署 EDR/MDR/SOC/DLP 等監控與應變處理。
2. 配合政府與金管會之零信任架構導入。
3. 配合與落實上市櫃資安指引的相關規範。
4. 落實 ISO 27001 與個資保護相關管理制度與成效。
5. 精進更完善的備份備援與復原機制。
6. 增加核心系統資安檢測之頻率，如：弱點掃描(包含源碼檢測，開源檢測，網頁弱掃)、滲透測試等。
7. 持續強化員工資安意識教育，增強社交工程演練效果與深度。
8. 根據資安攻防趨勢，持續投資先進的威脅偵測與資安防禦技術。

精誠資訊股份有限公司

代表人 林隆奮