資訊安全風險管理報告書

一、資訊安全政策

1. **目的**

   本公司制定此政策旨在透過系統化的風險評估方法，釐清資訊資產所面臨的風險，選擇適當方法進行風險管控，降低風險至可接受的程度，並確保資料、系統、設備及網路的安全，以持續提供穩定的資訊環境，符合相關法規，避免內部或外部蓄意或意外的威脅。

2. **適用範圍**

   - 涵蓋資訊機房、系統維護的安全管理，確保各項安全需求和期望的達成。
   - 涵蓋資訊記錄、業務、技術、財務、郵件、ERP、PLM、人事薪資及備份系統，防止資料不當使用、洩漏、竄改及破壞，並降低風險。
   - 包括防範內外部人員蓄意或過失洩漏公司機密資訊。
   - 涵蓋網路、通訊、電力、空調等設備與服務。
   - 所有內部人員、委外廠商與訪客需遵守此政策。

3. **目標**

   - 保護公司資訊資產的機密性、完整性及可用性，保障使用者資料隱私。
   - 建立跨部門的資訊安全組織，推動、實施及改進資訊安全管理。
   - 確保公司具備業務持續運作的資訊環境。
   - 提升資訊安全管理的有效性和即時性。

二、風險管理組織架構

1. **董事會**：委派具資訊專長的董事，負責公司內部資安風險管理的督導。
2. **總經理**：擔任總召集人，統籌風險管理計劃、檢討、修正及推行。
3. **資訊部門**：負責資訊資產的風險評估、員工資安教育訓練及內部稽核。

三、風險管理系統

1. **風險預防**：定期或不定期評估資通訊系統安全，並依據「資通安全風險管理程序」實施預防措施。

2. **緊急應變程序**：在資安預警系統偵測到可疑連線時，立刻啟動應變程序：
    - 確認受駭設備
    - 觀察連線情形
    - 採取中斷連線、停止網路服務等措施
3. **危機處理程序**：當發生資安事件時，啟動危機處理，以減少損失及保護公司資產。

四、資安與網路風險之評估

1. **資訊資產盤點**：鑑別資訊軟硬體資產，建立清冊。
2. **評價資訊資產**：以機密性、完整性、可用性三方面進行評估：
    - 機密性：根據使用權限進行分級，分為低、中、高、極高四個等級。
    - 可用性：評估授權者是否能在需要時正常存取資訊設備。
3. **鑑別威脅及脆弱點**：針對資產進行威脅及脆弱點的管理，並根據風險等級決定應對措施。
4. **資通安全風險管理評鑑表：**

NO	資產名稱	機密性	可用性	合計	威脅發生率	衝擊程度	風險等級
1	Nutanix	極高(4)	極高(4)	8	低(1)	低(1)	C(8)
2	ERP	極高(4)	極高(4)	8	低(1)	中(2)	C(18)
3	PLM	高(3)	高(3)	6	低(1)	中(2)	C(12)
4	Email	中(2)	中(2)	4	低(1)	低(1)	D(4)
5	人事薪資系統	高(3)	中(2)	6	低(1)	中(2)	C(12)
6	資訊備份系統	中(2)	低(1)	3	低(1)	低(1)	D(3)
7	防火牆	中(2)	高(3)	6	中(2)	低(1)	C(12)
8	MPLS VPN(網路語音)	中(2)	低(1)	3	低(1)	低(1)	D(3)
9	UPS	中(2)	低(1)	2	低(1)	低(1)	D(2)

五、資訊安全訓練

為提升本公司人員之資訊安全意識及認知，進行不定期 Email 社交工程演練。

2024/02：系統共發出 129 封電子信件，其中有 5 人點擊連結，2 人鍵入資料。

2024/05：系統共發出 127 封電子信件，所有人都成功通過測試。

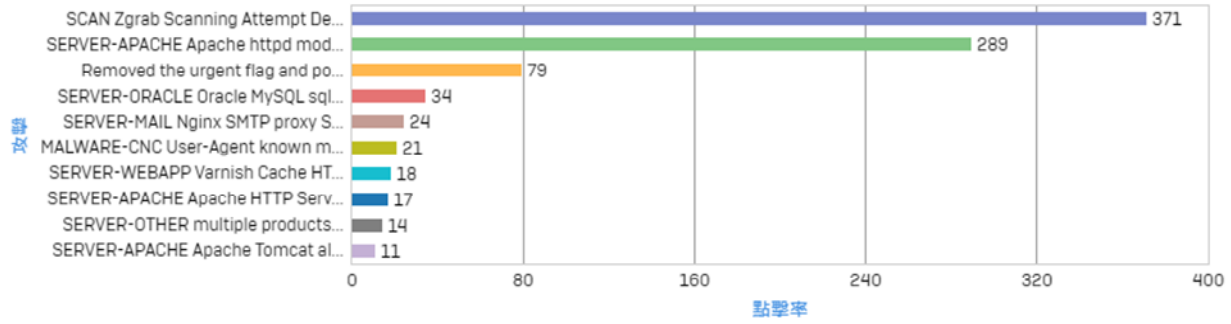
六、資訊安全所投入之資源

- 使用微軟 SPAM 降低收到釣魚郵件的機會
- 防火牆訂閱安全防護並更新系統
- 個人電腦安裝端點防毒軟體
- 進行資訊安全社交工程演練
- 導入 DLP 系統防止機密資料外洩

七、資訊安全事件

對外網頁 IP 每日皆會受到入侵攻擊，但皆被防火牆阻擋，因此未遭受到損害。

入侵攻擊



攻擊	點擊率
SCAN Zgrab Scanning Attempt Detected	371
SERVER-APACHE Apache httpd mod_http2 h2_session_process CVE-2023-43622 Denial of Service	289
Removed the urgent flag and pointer in TCP header	79
SERVER-ORACLE Oracle MySQL sql_authentication Integer Overflow	34
SERVER-MAIL Nginx SMTP proxy STARTTLS Plaintext CVE-2014-3556 Command Injection	24
MALWARE-CNC User-Agent known malicious user-agent string - Mirai	21
SERVER-WEBAPP Varnish Cache HTTP2 Flow Control CVE-2024-30156 Denial of Service	18
SERVER-APACHE Apache HTTP Server CVE-2021-41773 Path Traversal Vulnerability	17
SERVER-OTHER multiple products blacknurse ICMP denial of service attempt	14
SERVER-APACHE Apache Tomcat allowLinking URIencoding directory traversal attempt	11