經濟部

MOEAWRA1110390

111 年度工業控制系統(ICS)威脅偵測機制與資安演練服務

Industrial Control System (ICS) Threat Detection Mechanism and Security Drills Services of 2022

主辦機關：經濟部水利署南區水資源局

執行單位：松之安資訊科技有限公司

中　華　民　國　111　年　12　月

摘要

經濟部水利署南區水資源局所轄關鍵基礎設施場站為我國水資源領域重要關鍵基礎設施場站，為遵循資通安全管理法暨相關子法規範，並確保核心工業控制系統防護符合「經濟部能源及水資源領域工業控制系統資安防護基準」各項控制措施之要求，南區水資源局從政策面、管理面及技術面的防禦部署，並驗證及檢測相關資訊安全管理、防護機制的有效性，以維護和強化本局與轄管各關鍵基礎設施的資安防護，持續提升本局轄管水資源關鍵基礎設施場域面對可能資安事件衝擊的應對能力，建構嚴密之資通安全防護結構。

本計畫之工作包含建置基礎可視化網路監控平台(以曾文水庫與牡丹水庫2管理中心為範圍)及辦理曾文水庫管理中心紅隊演練，本團隊已於111年4月至11月期間，依工作執行計畫書進度陸續完成計畫相關工作項目，包括：

- 建置曾文水庫管理中心與牡丹水庫管理中心可視化監測平台，並持續蒐集主機狀態資訊與系統安全日誌，並舉辦可視化監測平台教育訓練，落實各項資安工作。
- 評估紅隊演練作業所需之情境場景，針對曾文水庫管理中心管理與維運人員進行訪談，並進行針對場域實體安全與內部網路安全進行評估。
- 已完成本年度曾文水庫管理中心紅隊演練作業，過程中發現相關的可能脆弱點與風險，並提出對應的矯正措施，進而提升本局資安防護能量。

結論與建議

本計畫自 111 年 04 月執行至今，各項工作皆按既定之期程順利執行，計畫團隊執行過程中適時與本局溝通協調，並依據相關回饋之意見調整執行細節，達成計畫相關目標。目前已於曾管中心與牡管中心建置可視化網路監控平台，蒐集工控主機設備狀態與系統日誌，透過可視化介面加強提供管理人員即時掌握各設備之資源與運轉狀態，進而確保系統持續營運。

本局首次在曾文水庫管理中心執行紅隊演練，透過紅隊演練形式驗證及檢視現有資訊安全管理及防護機制之有效性，提出持續改善及管理方式，強化本局所轄水資源場域資訊基礎設施防禦能量，以確保轄管關鍵基礎設施和重要資通系統的防護，達到保障經濟、民生穩定的重要目標。

評估本年度專案執行之各項工作與成果，建議局內相關單位及承辦人員除持續精進資安管控作為外，並需留意以下建議內容。

- 可視化監測平台已建置完成，透過平台可監測工控環境主機狀態與日誌蒐集呈現，建議管理人員仍須定期登入平台檢視主機設備狀態，並觀察相關主機安全日誌是否有異常行為。
- 有關 111 年度執行曾管中心紅隊演練作業，相關演練發現之短期矯正對策雖皆已完成，各單位仍須持續留意管控措施的落實，後續也須持續監測場域營運狀態與安全性，並強化各項管控措施作為，達到預防及降低風險的成效。

上述各項建議宜作為本局後續推行 ISMS 制度與遵循法令法規規範之重要事項之一，相信在局內同仁與委外廠商的協力推動下，應該順利推動，落實各項管控措施，符合資通安全管理法之要求，並確保本局核心業務的資安防護，保障區域的民生經濟發展。