CASE STUDY: Nuclear Waste Effluent Treatment Project

CHALLENGE

Our customer required their cybersecurity on their OT platforms to be enhanced to avoid potential cyber-attacks.

Bilfinger UK were awarded a contract to integrate a cybersecurity life cycle process into a traditional control system design to enable the customer to identify and remove any cyber related risks.

SOLUTION

- We executed a cybersecurity life cycle process in-line with IEC62443.
- We ensured the appropriate assessment of cyber risk.
- We implemented a number of chosen technologies according to risk.

BENEFITS | Removing Obsolescence | Enhancing Operations | Enhancing Supportability | Secure by Design |

Technical Information Summary

TECHNICAL MEASURES

Microsoft Windows

- Leverage Windows Active Directory – Enabling user administration, authentication and authorisation.
- Leverage Microsoft Security Baseline – Providing Microsoft recommended security configuration for windows based hosts.

Software Selection & Patch Management

- Software selection – Ensuring all software is supported for the life cycle of the facility along with migration paths for upgrades.
- Patch management – A critical part of an overall cybersecurity strategy. Install of latest patches during design lifecycle, ensuring all design, testing and commissioning. Provision of patch management instructions for all supplied devices ensuring easy integration into clients existing patch management process.

Secure Network Infrastructure

- Network segmentation & segregation – Utilising virtual LANS and traffic enforcement via security appliances.
- Loop prevention – Configuration of STP *(spanning tree protocol)*.
- Time synchronisation – Utilising NTP *(network time protocol)* for unified system logging.
- Secure access – Account access secured using encrypted usernames and passwords.

Device Hardening & Interface Restriction

- Disable all unused software enabled ports.
- All unused network ports placed in black hole VLAN.
- Physical port blockers used in tandem with software methods.
- Services and software installed only to support necessary functionality.

Integrated NMS

- Connection logging – Logging all traffic connections through security appliances.
- Intrusion detection – Detection and alerting using deep packet inspection against TALOS ruleset.
- Traffic restriction – Detection and alerting on all non authorised traffic.
- Port monitoring – Detection and alerting on all network ports.

Backup & Restore

- Processes – Detailed backup and restore processes that can be integrated into existing maintenance schedules and business continuity plans.