COME GARANTIRE FABBRICHE CONNESSE E SICURE?

AFFIDATI AI NOSTRI ESPERTI IN OT CYBER SECURITY

SERVIZI DI SICUREZZA INFORMATICA OT PER **COSTRUTTORI DI MACCHINE E SYSTEM INTEGRATOR**

Vulnerability Assesment di sistemi OT

Attraverso strumenti specifici per l'ambiente industriale e utilizzando le modalità black box o white box vengono rilevate le vulnerabilità esistenti e prioritizzate nella realtà del cliente. Al termine delle attività viene redatto un report contenente le vulnerabilità riscontrate e possibili contromisure da adottare. Viene dunque discusso il report con il cliente.

Penetration Test sistemi OT

Attraverso strumenti specifici per l'ambiente industriale o con azioni guidate dallo specialista vengono testate le vulnerabilità riscontrate al fine di dimostrare l'effettiva vulnerabilità del sistema oggetto del Penetration test. Al termine delle attività viene redatto un report contenete le vulnerabilità riscontrate e possibili contromisure da adottare. Viene dunque discusso il report con il cliente.

Consulenza OT Security e IEC 62443

Attraverso consulenti certificati viene condotto, con il supporto del Cliente, un assessment utilizzando i requisiti e la metodologia richiesta da ISA/IEC 62443 per facilitare il processo di certificazione. In caso di non conformità lo specialista suggerirà le adeguate azioni correttive.

Lapp Italia Srl | Via Lavoratori Autobianchi, 1 - Desio (MB)
+39 0362 4871 | marketing.it.lit@lapp.com | www.lappitalia.com

COME GARANTIRE FABBRICHE CONNESSE E SICURE?

AFFIDATI AI NOSTRI ESPERTI IN OT CYBER SECURITY

SERVIZI DI SICUREZZA INFORMATICA OT PER **UTILIZZATORI FINALI**

Oltre ai servizi previsti per i system integrator che possono essere proposti anche per gli utilizzatori finali sono previsti i seguenti servizi:

Risk Management

- **Definizione del Perimetro:** Identificare e definire l'ambito del sistema di automazione e controllo industriale (IACS) che sarà oggetto dell'assessment.
- **Valutazione iniziale dei Rischi:** Condurre una valutazione dei rischi identificando gli asset e le minacce afferenti al fine di identificare il rischio in ambito OT.
- **Valutazione delle contromisure** che consentono di colmare i GAP tra il rischio rilevato ed il rischio atteso/accettato.
- I requisiti di cybersecurity possono essere valutati rispetto alle norme di riferimento quali: **ISA/IEC 62443, Regolamento Macchine UE 1230/2023, Direttiva NIS 2, Cyber Resilience Act e ISO 27001.**

Continuous Vulnerability Assessment: verificare continuamente attraverso apposite sonde specifiche per gli ambienti industriali l'aderenza allo standard ISA/IEC 62443.

Security Monitor: attraverso un SOC attivo H24 è possibile monitorare gli eventi di sicurezza ed indirizzare in modo tempestivo eventuali problemi.

Segmentazione di rete: progettazione ed eventuale realizzazione di una rete segmentata adeguata a supportare Zone e Conduit secondo lo standard ISA/IEC 62443.

Security Awareness: formazione specifica in ambito Cybersecurity.

Lapp Italia Srl | Via Lavoratori Autobianchi, 1 - Desio (MB)
+39 0362 4871 | marketing.it.lit@lapp.com | www.lappitalia.com