POLO TECNOLOGICO
ALTO ADRIATICO

Incubatore certificato dal Ministero delle Imprese e del Made in Italy

BUSINESS UNIT CYBERSECURITY

La Cybersecurity è essenziale nell'era digitale per proteggere dati sensibili e infrastrutture critiche. Affronta sofisticate minacce informatiche, salvaguarda la privacy, assicura operazioni sicure in rete e rafforza la fiducia nel progresso tecnologico, cruciale per società e economia.

Il Polo Tecnologico Alto Adriatico è da tempo impegnato sui temi della Cybersecurity per la quale è stata costituita una specifica Business Unit, da tempo coinvolta in progetti nazionali e internazionali. Coerentemente con il modello KIBS (Knowledge Intensive Business Services), il Polo Tecnologico è a disposizione per accompagnare organizzazioni private e pubbliche nel percorso verso l'adozione consapevole di soluzioni di Cybersecurity, grazie a un team costituito da professionisti interni qualificati e da una fitta rete di partner con competenze verticali sui diversi aspetti della Cybersecurity.

www.polotecnologicoaltoadriatico.it

A CHI CI RIVOLGIAMO

Ad aziende e istituzioni che vogliano migliorare la sicurezza nel trattamento dei dati e delle informazioni presenti in azienda con un approccio basato su aspetti procedurali e tecnologici.

T +39 0434 504411
direzione@poloaa.it
polotecnologicoaltoadriatico.it

READY! TO-GO

POLO TECNOLOGICO
ALTO ADRIATICO

CYBERSECURITY

READY TO-GO!

I dati sono un valore inestimabile.
Il Polo B.U. Cyber Security
ti aiuta a proteggerli.

ASSESSMENT CYBERSECURITY / PRIVACY

Basato su checklist ENISA, comprende controlli CyberSecurity e Privacy relativi ai seguenti aspetti:

- Tecnologici
- Procedurali
- Legali

L'assessment viene proposto in tre livelli a complessità crescente, da erogarsi in tre momenti differenti: Base, Intermedio e Avanzato.Al termine dell'assessment viene rilasciato un verbale di audit che costituisce guida per l'implementazione dei punti rilevati come non conformi o critici. Tale percorso di adeguamento può venire portato a compimento in modo autonomo dall'azienda o tramite un'attività di accompagnamento.

ACCOMPAGNAMENTO ALL'ADOZIONE DI BEST PRATICES CYBERSECURITY / PRIVACY

L'attività comprende un percorso di accompagnamento e supervisione volto a supportare l'azienda nell'adozione delle migliori pratiche in materia di Cybersecurity / Privacy.

ASSESSMENT PER RETI IT / OT

Particolarmente adatto per aziende che hanno già intrapreso il percorso Industria 4.0 / Transizione 4.0 per proteggere le reti IT oltre alle reti della fabbrica.

VULNERABILITY ASSESSMENT

La continua diffusione di Virus, Trojan, Malware e soprattutto Ransomware, induce gli amministratori di rete a porsi seriamente una domanda: la rete aziendale è al sicuro?

Certamente le possibilità di penetrazione sono molteplici. Tuttavia, il controllo delle vulnerabilità di base della propria rete aziendale, è tra i precisi doveri di un amministratore di rete.

Non è sufficiente proteggersi con un firewall: le regole infatti potrebbero non essere adeguate, o il firmware del firewall potrebbe essere obsoleto. Oppure potrebbe esserci un antivirus non aggiornato o non adeguato. O ancora, potrebbe esserci un sistema operativo contenente una vulnerabilità nota, che potrebbe quindi compromettere la sicurezza dell'intera azienda. Anche in modo grave, magari causando dei pericolosi fermi macchina.

L'alta disponibilità dei servizi oggi è fondamentale per competere in un mercato dinamico.
Ecco perché è fondamentale valutare la sicurezza della rete aziendale con un Vulnerability Assessment. Sostanzialmente si tratta di una ricerca di vulnerabilità controllata, effettuata da alcuni software, allo scopo di valutare le vulnerabilità della rete aziendale.

CYBERSECURITY PER PRODUTTORI IMPIANTI/SOFTWARE

Le tematiche della Cybersecurity oggi impattano significativamente anche sulle attività dei produttori impianti così come di software. L'implementazione della cybersecurity offre vantaggi significativi agli stessi produttori. Infatti:

- aumenta la fiducia dei clienti, garantendo la protezione dei dati e la continuità operativa
- riduce il rischio di attacchi informatici e violazioni di dati, minimizzando i costi legali e di ripristino
- migliora la competitività, assicurando conformità alle normative
- rafforza la resilienza operativa, ottimizzando l'uptime e la produttività

In definitiva consente di ampliare il portafoglio dei propri clienti garantendo prodotti / servizi sicuri ed efficienti.

MONITORAGGIO REAL TIME DI INFRASTRUTTURE DI RETE

L'adozione di un Security Operation Center (SOC) offre numerosi vantaggi, tra i quali, il monitoraggio costante delle minacce, consentendo una risposta rapida agli incidenti di sicurezza. Nel contempo, migliora la visibilità delle reti e dei sistemi, identificando vulnerabilità e gli eventuali attacchi in corso.

Nondimeno aumenta l'efficienza nella gestione della sicurezza, centralizzando operazioni e risorse e riduce i rischi di violazioni di dati e le relative sanzioni. Infine, rafforza la compliance con le normative di settore e migliora la fiducia dei clienti.

POLO TECNOLOGICO
ALTO ADRIATICO

Un'azienda avrà una buona sicurezza se ci sono delle buone direttive del top management.

Non ci potrà essere alcuno sforzo operativo per superare la negligenza aziendale.
William "Bill" Malik, Vice President Gartner

Polo Tecnologico Alto Adriatico
Società Benefit
Andrea Galvani SCpA
via Roveredo, 20/b
33170 Pordenone

Italia