Aziende & Territorio

a cura di PUBLIMEDIAGROUP.IT

Il futuro digitale è ora: le imprese che sfidano i confini della tecnologia

Universi digitali che cambiano il modo di lavorare e di produrre: dall'IA all'IoT, dal cloud al ML, il business è sempre più intelligente.

Il PNRR ha messo al centro dell'attenzione l'importanza, per le aziende, di digitalizzare i processi e far propri nuovi modelli di business. La Digital Transformation implica una rivoluzione culturale che spinge il mondo produttivo a "pensare digitale" e che trova nel tessuto imprenditoriale italiano terreno fertile e ricco di realtà all'avanguardia che comprendono le nuove esigenze dell'industria, del manifatturiero, dei servizi e rispondono con soluzioni tecnologiche ad hoc. Innovazione e vision lungimirante sono i driver che permettono all'imprenditoria 4.0 di generare valore e competitività.

www.securitymind.cloud

Security Mind: cybersecurity, psicologia comportamentale e comunicazione per difendersi dalle cyber-minacce

In un contesto digitale in costante evoluzione, dove le minacce informatiche diventano più sofisticate, garantire la conformità alla direttiva NIS2 rappresenta una sfida strategica. **Security Mind** è progettata per rivoluzionare la cultura della sicurezza, supportando le Aziende nella protezione del proprio ecosistema digitale e aiutando a costruire una consapevolezza duratura, grazie ad un approccio integrato che combina Cybersecurity, Psicologia Comportamentale e Comunicazione. Le nuove normative introducono standard di sicurezza più elevati e la tecnologia da sola è insufficiente: il fattore umano rimane il punto più vulnerabile, il 90% degli attacchi informatici riesce a causa di un errore umano. Il metodo di Security Mind si ispira anche al modello di Paul MacLean, che distingue 3 aree del cervello: rettiliano, che reagisce istintivamente ai pericoli, spingendoci ad agire d'impulso, un meccanismo sfruttato nel phishing; limbico, che gestisce emozioni e relazioni, esponendoci a manipolazioni basate su paura, urgenza o fiducia; neocorticale: sede del pensiero razionale, indispensabile per riconoscere le minacce e prendere decisioni consapevoli. Comprendere queste dinamiche consente di sviluppare percorsi di Cyber Awareness più efficaci, in grado di rafforzare la capacità di risposta degli utenti e ridurre i rischi aziendali. Veronica Patron, co-fondatrice di Security Mind, sottolinea che investire nella consapevolezza significa investire nella sicurezza a tutti i livelli. Info: securitymind.cloud

I "must have" per la protezione delle infrastrutture industriali

Longwave implementa le soluzioni Cisco per innalzare il livello di cybersecurity nel manifatturiero

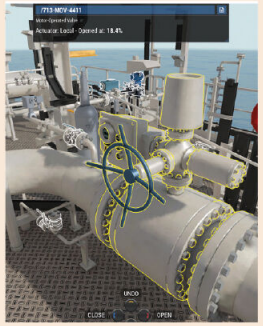
Il manifatturiero sempre più nel mirino dei cybercriminali: si può riassumere così il preoccupante ritratto della cybersecurity in Italia emerso dal rapporto Clusit 2024. Un settore, quello industriale, che è ancora oggi tra i più colpiti, rappresentando il target di un quarto degli attacchi OT a livello globale, con una crescita costante dal 2019. Solo l'1% delle violazioni ha avuto un impatto basso e le conseguenze economiche sono spesso state devastanti. Ma perché queste aziende sono il bersaglio preferito degli hacker? Cosa dovrebbero fare per fronteggiare ad armi pari la criminalità informatica? Spesso dotate di infrastrutture obsolete ed alcune da un'eccessiva "pigrizia" nell'adoption di percorsi migliorativi, la priorità è quasi sempre la produzione, con una ridotta cultura della sicurezza e sensibilità al tema. Non è un caso che gli attacchi phishing vadano spesso a segno: in Italia sono cresciuti dell'87% nell'ultimo anno. Il paradigma che le industrie dovrebbero adottare prevede alcuni "must have", delle strategie fondamentali per ridurre la superficie esposta e mettere in sicurezza le infrastrutture. In primis, è indispensabile poter contare su un monitoraggio proattivo e un'analisi continua del traffico OT per rilevare immediatamente vulnerabilità, anomalie e potenziali minacce e soprattutto rispondere in maniera tempestiva. L'analisi puntuale e la raccolta delle informazioni sulle minacce emergenti tramite sistemi di Threat Intelligence è la chiave di volta per anticipare i potenziali attaccanti. Un altro aspetto "must have" è sicuramente la segmentazione della rete e la gestione delle identity per il controllo degli accessi: creare segmenti di rete sicuri, separando i sistemi OT dalle reti IT consente di mitigare il rischio attacco, isolando le zone compromesse e mantenendo operative quelle "sane". Non meno importante è la formazione del personale in materia di cybersecurity. Creare una cultura della sicurezza all'interno dell'azienda è fondamentale per riconoscere comportamenti sospetti e non cadere nelle trappole del social engineering. Longwave implementa tecnologie Cisco come Secure Firewall, Identity Service Engine, Cybervision e la piattaforma di orchestrazione SecureX per garantire che questi fattori siano sempre presenti e ottimizzati in ogni progetto di Cybersecurity OT. Adottando un modello Zero Trust e un approccio basato su assessment, GAP Analysis e remediation plan strutturati, completati da servizi di awareness, governance e threat management, la gestione della sicurezza in ambito OT è impostata ciclicamente per non lasciare mai scampo ai cybercriminali. Info: www.longwave.it

Longwave CISCO Gold Integrator Partner

F. Grasso: Business Manager Security

LION® Cybersecurity: management H24

LION® è la suite di servizi gestiti di Longwave per il monitoring e la gestione H24 7/7 dell'intera infrastruttura IT.



Digital Twin 3D

Kairos3D guida l'industria nei Digital Twin 3D

Kairos3D, specializzata nello sviluppo di soluzioni 3D interattive in tempo reale, sta rivoluzionando il modo in cui le aziende gestiscono i Digital Twin industriali. Grazie alla piattaforma Gilgamesh, le imprese possono visualizzare, analizzare e interagire con i propri dati in ambienti 3D immersivi, senza bisogno di competenze di programmazione. Nata con un focus su Oil&Gas ed energia, oggi Kairos3D opera in settori strategici come manifatturiero, trasporti, scienze della vita, costruzioni, aerospaziale e automotive, offrendo soluzioni per formazione immersiva, manutenzione, sicurezza e ingegneria. Kairos3D aiuta le aziende a ridurre costi e complessità, accelerando la trasformazione digitale e portando l'Industria 4.0 ad un livello superiore. Info: www.kairos3d.it

www.iridesgroup.it

Iridesgroup, la tecnologia diventa a misura di cliente

Iridesgroup dal 2001 unisce la tradizione sartoriale biellese con le moderne innovazioni digitali disegnate ad arte per trasformare singoli servizi in obiettivi realizzati per il cliente: qui la realtà non è uno slogan "preconfezionato". La filosofia è quella di un approccio ideato ed organizzato in modo flessibile, sicuro e sostenibile: l'azienda si distingue per formazione e investimento costante, realizzando servizi in cybersicurezza, networking, telecomunicazione e cloud. Il modello aziendale è guidato da Laura Festa Rovera e Paolo Montarolo, che hanno creato con lungimiranza un team di lavoro che oggi esprime il suo potenziale nelle tecnologie digitali, valorizzando il fattore umano per il successo dei propri clienti. Info: www.iridesgroup.it