Non c’è safety senza cybersecurity:

A Piacenza MindSphere World chiude l’evento dedicato alla sicurezza delle macchine e impianti industriali

Piacenza, 05 aprile – Si è concluso ieri l’evento “**Macchine Protette – non c’è più safety senza cybersecurity**” promosso da **MindSphere World** a Piacenza. L’Associazione - che dal 2018 si fa promotrice dello sviluppo digitale del settore industriale e che riunisce un network di professionisti dell’IT, dell’OT ed esperti di automazione industriale - ha affrontato il tema della *cybersecurity* con **enti istituzionali**, **Associazioni di categoria**, **Competence Center** e professionisti di alto profilo come il **Generale Paolo Poletti** – Presidente di Securitalia Security Solutions ed ex Vicedirettore dell'Agenzia Informazioni e Sicurezza Esterna (AIS). Una serie di incontri lungo tutta la giornata che hanno permesso ai partecipanti di approfondire in maniera eterogenea le **norme**, le **competenze** e gli **strumenti** utili ad alzare il livello di sicurezza delle reti.

Macchine Protette è stato inaugurato dall’intervento del **Generale Poletti** che, in considerazione dalle recenti ricerche su scala globale che vedono **Government (20%)** e **Manufacturing (19%)** come le categorie maggiormente colpite da cyber attack su territorio italiano**,** ha sottolineato come gli attacchi cyber sono per lo più compiuti da gruppi di competitor o enti governativi di altri Paesi. Lo scopo è principalmente quello di *indebolire il Sistema Paese e di intercettare il know-how delle realtà imprenditoriali*. Il motivo è che l’industria è il settore d’avanguardia che traina l’economia mondiale e “*nessuno può permettersi di rimanere indietro*”, conferma il Generale Poletti. Il Presidente di Securitalia ha poi evidenziato come presto, oltre al comparto industriale, anche la **sanità** dovrà necessariamente adeguarsi e investire sulla cybersecurity, in previsione della futura telemedicina che porterà ad un’interconnessione dei macchinari e dei sistemi di gestione di tutto il settore. Un trend inevitabile che richiede sicurezza per garantire un elevato ed ottimale stato di safety. Si ricordi che nel mondo a causa di attacchi hacker ci sono stati incidenti sanitari che hanno portato a gravi conseguenze come la morte di alcuni pazienti.

Non c’è dunque safety senza cybersecurity, e gli **investimenti europei e di Paesi extraeuropei** confermano questa posizione. È infatti previsto **che il mercato globale passerà dai 133,3 miliardi di dollari di investimenti nella protezione delle infrastrutture critiche del 2021 a 157,1 miliardi entro il 2026**. Investimenti che devono andare di pari passo con *standard normativi* che mettano in sicurezza costruttori di macchine ed end user. Ecco perché durante la giornata è stato approfondito anche l’aspetto legale. Lo **Studio Legale Oddo Lora Gabriele** ha presentato alla platea le direttive promosse dal **Nuovo Regolamento Macchine** – che si riferisce principalmente alla sicurezza dei macchinari - e dal **NIS (Network and Information System) 2**– che fa riferimento all’affidabilità dei servizi industriali. Queste due normative hanno l’obiettivo di salvaguardare l’integrità della macchina e del dato per garantire un elevato livello di safety. In particolare, nel NIS 2 si parla di affidabilità in termini di sicurezza del software, dell’importanza dell’analisi dei rischi, dei termini essenziali di individuazione

delle responsabilità e della proprietà dei dati. Questo a dimostrazione della diretta interconnessione tra OT e IT, che oggi definisce l'Industry 4.0.

A seguire sono poi intervenuti esponenti di Associazioni di categoria come **ANIPLA, UCIMA e UCIMU**. Oltre ad aziende abilitatrici del digitale nel comparto. Una giornata che ha riscosso un grande successo in termini di partecipazione e di interesse, risultato dell'importanza del tema e della necessità di approfondirlo per l'ottimizzazione di una fabbrica d'avanguardia.

Massimo Veronesi, Consigliere di **ANIPLA** ha commentato: "*Le intrusioni esterne nelle reti aziendali sono ormai all'ordine del giorno nel contesto di crescenti tensioni internazionali, in cui organizzazioni senza scrupoli usano ogni mezzo per trarre vantaggi per sé o causare problemi ad altri. Le infrastrutture industriali critiche hanno quindi da anni iniziato a difendersi per non pregiudicare la produttività e la sicurezza dell'impianto. Sull'altro fronte però la condivisione dei dati relativi all'esercizio è diventato un fattore chiave per la gestione della produzione, la cui ottimizzazione è sempre più opportuna per assicurare la necessaria competitività internazionale. Risulta pertanto necessario trovare l'equilibrio più adatto in grado di bilanciare le esigenze di informazioni con quelle di sicurezza. In questo contesto gli IEC-Standard di riferimento per la Safety e la Security costituiscono una solida base sulla quale costruire la robustezza (tecnica e procedurale) necessaria per ridurre il rischio di incidenti, o difendere ciò che è stato fatto qualora si verificassero*".

Matteo Marconi, Consulente su normativa, sicurezza ed export di **UCIMA**, è poi entrato nel dettaglio dei dati rilevati a livello nazionale affermando: "*È chiaro che ci troviamo sotto una nuova forma di attacco alle aziende, è sotto gli occhi di tutti, ma dobbiamo leggere questo incremento esponenziale degli attacchi informatici anche in un'altra ottica, quella Industriale, non solo IT ma nel mondo OT. Gli operatori e tecnici IT e OT devono collaborare! Il 94% degli attacchi a sistemi IT ha portato anche a blocchi nei sistemi OT, che significa blocchi di produzione e quindi fabbriche, linee ferme, per una mancanza o troppa integrazione non gestita tra le reti IT ed OT. Viceversa. un accesso dalla rete OT delle macchine, ormai tutte interconnesse e dotate di sistemi di assistenza remota, può portare ad una invasione del mondo IT*".

"*UCIMU - SISTEMI PER PRODURRE, così come le sue Aziende Associate, ritiene che la sostenibilità - economica, sociale ed ambientale - sia un valore irrinunciabile per il settore italiano della macchina utensile. Rinunciare alla sicurezza significa minare alla base tale valore, sia per quanto riguarda il valore dato dalla componente fisica del manifatturiero, sia per quanto riguarda la sua componente digitale, con impatto sulla efficacia, l'efficienza e la resilienza delle aziende (fornitrici o utilizzatrici di macchine) e dell'economia nazionale*" ha concluso poi il Responsabile della Direzione Tecnica di **UCIMU**, **Enrico Annacondia**

Andrea Gozzi, Segretario Generale di MindSphere World ha poi concluso "*la grande partecipazione di pubblico a Macchine Protette dimostra quanto il tema della cybersecurity sia sentito dal mondo dell'industria. Con la nostra Associazione abbiamo voluto rispondere a questa necessità e ci siamo attivati per supportare il mercato delle macchine e impianti industriali nel*

processo di adozione di buone pratiche e di buone tecnologie per la sicurezza informatica. A Macchine Protette abbiamo imparato che i costruttori di macchine devono riorganizzarsi per offrire servizi efficaci al mercato, ed in alcuni casi obbligatori secondo le nuove normative. Come la distribuzione di aggiornamenti di sicurezza informatica per gli impianti, o la certificazione della affidabilità, anche dal punto di vista cibernetico, dei loro fornitori. Di grande utilità sono state le indicazioni ricevute dagli esperti intervenuti in merito all'importanza della formazione del personale e della gestione degli aspetti legali e contrattuali considerando anche il rischio di un data breach che si può propagare verso i propri clienti".

Media Partner dell'evento

Ufficio Stampa MindSphere World

Maria Grazia Persico – mgpersico@mgpcomunicazione.it – cell. 335 64 69 568
Ingrid Paron – press@mgpcomunicazione.it – cell. 391 73 60 094

MindSphere World Italia

Via Vipiteno, 4 20128 Milano – Italia

info@mindsphereworld.it

www.mindsphereworld.org

MindSphere World

MindSphere World è una comunità globale di aziende e istituti di ricerca nata per modellare insieme il futuro dell'Internet of Things Industriale (IIoT). Unire le forze e condividere le esperienze permette ai soci di stare al passo con il mondo digitale in rapida evoluzione. MindSphere World è stato fondato nel 2018 da Siemens insieme a 18 aziende leader del settore industriale per dare voce alle imprese che utilizzano e sviluppano le loro soluzioni basate su MindSphere, la principale soluzione di IoT Industriale "as-a-service" basata sul modello di ecosistema. Da allora si è espansa in un'ampia comunità che include lo sviluppo di modelli di business, proposte sui requisiti tecnici così come raccomandazioni per creare regole uniformi per l'uso dei dati. L'associazione promuove anche lo studio e la ricerca intorno all'Industrial IoT. MindSphere World comprende sette associazioni regionali in Europa, Asia-Pacifico e Nord America e conta 170 soci nel mondo.