Tecnologia - *Cybersecurity e AI, i pilastri del futuro digitale protagonisti a Roma per Cybertech Europe 2025*

Roma - 27 ott 2025 (Prima Notizia 24) **L'ottava edizione si è svolta al Centro Congressi La Nuvola. Tra gli ospiti, l'ex Segretario di Stato Usa Mike Pompeo.**

Si è conclusa presso il Centro Congressi La Nuvola di Roma, l'ottava edizione di Cybertech Europe, il principale evento europeo dedicato alla cybersecurity e all'innovazione digitale. L'edizione 2025 ha confermato come la cybersecurity sia ormai un fattore strategico della trasformazione digitale, non più soltanto un ambito tecnico ma una leva essenziale per la resilienza economica e sociale. Nel corso dei panel tematici è emerso con chiarezza come intelligenza artificiale e tecnologie quantistiche costituiscano oggi i pilastri della nuova sicurezza digitale: l'AI, in particolare, sta rivoluzionando tanto le strategie di difesa quanto le tecniche di attacchi cyber, offrendo strumenti di rilevamento sempre più avanzati ma anche nuove potenziali vulnerabilità legate a un uso improprio della tecnologia. Durante i due giorni di lavori, leader internazionali, rappresentanti istituzionali, CISO e innovatori hanno affrontato e discusso i temi più rilevanti e innovativi del settore delineando le priorità per il futuro della sicurezza digitale nel mondo. Tra gli interventi più attesi, quello di Mike Pompeo, ex Segretario di Stato degli Stati Uniti (2018–2021) e Direttore della CIA (2017–2018), che ha offerto una visione approfondita sul ruolo centrale della cybersecurity nel nuovo scenario globale. Ripercorrendo le sfide affrontate durante il suo mandato, Pompeo ha sottolineato come gli Stati Uniti continuino a rappresentare un motore di innovazione, tanto in ambito militare quanto strategico, ponendo la tecnologia al centro delle dinamiche di sicurezza e di potere internazionale. Pur riconoscendo l'esistenza di differenze tra le due sponde dell'Atlantico, Pompeo ha definito la relazione tra Stati Uniti e Unione Europea "intatta e destinata a durare", richiamando i valori fondamentali condivisi e ribadendo che la collaborazione transatlantica resta essenziale per affrontare le minacce provenienti dalle potenze autoritarie. L'ex Segretario di Stato ha inoltre evidenziato come l'intelligenza artificiale si appresti ad assumere un ruolo sempre più rilevante non solo nella cybersicurezza, ma in ogni settore strategico, con impatti significativi sugli equilibri geopolitici e sull'economia mondiale. Pompeo ha infine richiamato l'Europa alla necessità di ridurre la burocrazia per favorire l'innovazione, invitando le istituzioni a "premiare gli innovatori" e a costruire "un ecosistema tecnologico senza rivali nel mondo". Con oltre migliaia di partecipanti provenienti da tutto il mondo, decine di sessioni dedicate alle tecnologie emergenti e un network in continua espansione, Cybertech Europe si conferma anche quest'anno un hub strategico per il dialogo globale sulla sicurezza digitale riaffermando l'importanza di un approccio sistemico alla sicurezza digitale. La crescita costante dell'evento testimonia non solo l'urgenza del tema, ma anche la capacità dell'Italia di porsi al centro della scena europea come promotrice di innovazione,

collaborazione e leadership nel settore cyber.“Cybertech Europe – ha detto Michele Lamartina, Regional Vice President Italia, Grecia, Cipro & Malta di Palo Alto Networks - si conferma, ancora una volta, l’appuntamento di riferimento in Italia per il settore della cybersecurity. Le sessioni che si sono susseguite nei due giorni e i momenti di confronto con i C-level italiani hanno ribadito con chiarezza come l’adozione di tecnologie avanzate, la spinta all’innovazione e la capacità di trasformazione siano oggi pilastri irrinunciabili per ogni azienda. È pertanto fondamentale che la sicurezza non sia percepita unicamente come una priorità, ma si elevi a responsabilità collettiva, condivisa e diffusa a tutti i livelli aziendali. Si tratta di un approccio essenziale per garantire un progresso digitale sicuro, un futuro resiliente agli attacchi e per contrastare in modo efficace gruppi e tecniche criminali sempre più evoluti e pericolosi. L’integrazione strategica dell’intelligenza artificiale è ora fondamentale per potenziare queste tecnologie avanzate, fornendo insight automatizzati, capacità predittiva e risposte rapide necessarie per neutralizzare queste minacce in evoluzione con velocità e precisione senza precedenti”. “La presenza di Eset a Cybertech Europe 2025, per il secondo anno consecutivo, rappresenta un momento significativo per riaffermare il nostro impegno nel promuovere una cultura della sicurezza informatica evoluta e consapevole. In un contesto digitale sempre più esposto a minacce sofisticate, è fondamentale che le organizzazioni, dalle piccole e medie aziende fino alle grandi enterprise, adottino soluzioni avanzate in cui i servizi MDR e le piattaforme di Threat Intelligence rappresentino dei veri strumenti strategici per garantire la protezione del dato, la continuità operativa e la resilienza aziendale. In questo contesto, Eset si presenta quindi come un attore autorevole e strategico nel panorama internazionale della cybersecurity, con un ruolo attivo e propositivo nel supportare le aziende, promuovendo l’adozione dei servizi MDR come pilastro fondamentale nella costruzione della postura di sicurezza da parte di clienti e partner”, ha dichiarato Fabio Buccigrossi, Country Manager Eset Italia.Salvatore Frosina, Co-Ceo di Dgs, ha detto: “In uno scenario digitale sempre più interconnesso la cybersecurity non può essere frammentata: serve un ecosistema collaborativo. È proprio da questa consapevolezza che nasce l’iniziativa “DGS CyberMesh”, con cui abbiamo portato al Cybertech una visione olistica della cybersecurity, costruita insieme a oltre 40 partner tecnologici e fondata su tre pilastri strategici: Managed Security Services, Cyber Resilience & Defense, e Foundation Security. Un approccio incentrato sul paradigma Cybersecurity Mesh Architecture (CSMA), pensato per affrontare con successo le sfide di ambienti IT sempre più interoperabili. Attraverso l’eXtended Security Operation Center (X-SOC), i nostri laboratori d’innovazione (i DGS CyLABs) e un approccio prevention first, offriamo servizi concreti e soluzioni su misura per garantire continuità, scalabilità e fiducia. DGS è al fianco delle organizzazioni per trasformare la sicurezza in un vantaggio competitivo”.“Al cuore di Cybertech Europe – ha sottolineato Cristiano Voschion, Country Manager Italy di Check Point Software Technologies - c’è una sfida condivisa: allineare la sicurezza al ritmo dell’innovazione guidata dall’AI, senza frenare l’innovazione. In collaborazione con Amazon Web Services (AWS), abbiamo mostrato come un modello di sicurezza prevention-first, nativamente integrato dal cloud alla rete, ai data center e agli endpoint, permetta alle imprese di accelerare e competere in modo sicuro. La storyline di Check Point “Securing the Hyperconnected AI-Driven World” si declina in quattro pilastri coerenti: Security for Hybrid Mesh

Networks, sicurezza per la forza lavoro, per la trasformazione dell'AI e Prevention-First Security. Il takeaway condiviso all'evento romano è chiaro: le organizzazioni chiedono piattaforme unificate, automazione intelligente e competenze per trasformare la complessità in resilienza. Con oltre trent'anni di esperienza e un ecosistema di partner, Check Point è al fianco del sistema-Paese per rendere la trasformazione digitale più sicura e sostenibile". Vittorio Bitteleri, Country Manager Italia di Cyber Guru, ha dichiarato: "La partecipazione a Cybertech Europe 2025 è per noi un passaggio chiave: conferma che la cybersecurity non è più un'area tecnica specialistica, ma un elemento strategico della trasformazione digitale e della governance aziendale. Quest'anno sul palco è andata in scena la nostra visione evoluta, il nuovo metodo formativo 'e-volve': formazione continua, coinvolgimento concreto e supporto in tempo reale per costruire una cultura della sicurezza quotidiana. Le soluzioni che abbiamo presentato, dall'Awareness Training alla Real Time Awareness fino al nuovo Cyber Advisor, sono infatti pensate per tradurre concetti complessi e trasformali in comportamenti misurabili e permanenti. La grande affluenza all'evento conferma che il mercato è pronto per questo cambio di paradigma: la vera rivoluzione nella cybersecurity non arriva dal codice, ma dal cervello. Ed è lì che noi di Cyber Guru lavoriamo ogni giorno, trasformando ogni dipendente da potenziale vulnerabilità a difesa attiva". "Il Cybertech Europe – ha detto Salvatore Marcis, Country Manager Trend Micro Italia - è sempre un momento di riferimento per l'intera industry della cybersecurity ed è un'occasione unica che permette a istituzioni, organizzazioni private e realtà globali di incontrarsi e condividere esperienze, con l'obiettivo di fare squadra contro le minacce e riflettere sul futuro della sicurezza informatica, a livello di sistema. Come Trend Micro, grazie alla nostra vision incentrata su un approccio integrato, proattivo e potenziato dall'intelligenza artificiale, siamo sempre pronti a supportare specialisti, aziende ed enti pubblici nel prevedere e prevenire le minacce, moltiplicando la capacità di azione e semplificando le operazioni". "La sicurezza informatica – ha sottolineato Cristiano Tito, Cyber Security Services Portfolio Lead, IBM Italy - sta entrando in una nuova era, caratterizzata da una doppia rivoluzione: intelligenza artificiale e informatica quantistica. Chi saprà integrare l'AI e il quantum computing come strumenti sinergici avrà la possibilità di rinforzare le proprie capacità di rilevamento, resilienza e risposta a eventuali attacchi. Allo stesso tempo, è necessario non perdere di vista la dimensione geopolitica: chi sarà all'avanguardia in queste due tecnologie plasmerà il futuro della sicurezza informatica". Emilio Turani, Managing Director per Italia, South Eastern Europe, Turchia e Grecia di Qualys, ha dichiarato: "La cybersecurity oggi si trova di fronte a un panorama sempre più complesso e sfidante, dove non basta più reagire agli incidenti ma è necessario anticipare i rischi in modo proattivo. In Qualys, crediamo che la sicurezza debba essere un elemento strutturale del valore digitale di ogni impresa, integrata nei processi e nella governance del rischio. A Cybertech abbiamo presentato il nostro approccio Risk Operations Center (ROC) che rappresenta un'evoluzione fondamentale, offrendo una visibilità continua e una prioritizzazione basata sul contesto di business, permettendo di tradurre vulnerabilità in decisioni operative efficaci. Grazie all'innovazione dell'Agentic AI, siamo in grado di automatizzare la gestione del rischio cyber con agenti autonomi che anticipano, correlano e rispondono alle minacce in tempo reale, trasformando la cybersecurity da funzione IT a funzione strategica di governance e resilienza".

“Cybertech Europe 2025 rappresenta un’occasione fondamentale per approfondire il dialogo su come possiamo, insieme, rafforzare la resilienza digitale in un’epoca segnata dalle minacce guidate dall’intelligenza artificiale – sono le parole di Rob Harrison, SVP Product Management Sophos -. In Sophos crediamo che una cybersecurity efficace si fondi su intelligenza, innovazione e collaborazione. Condividendo la nostra esperienza e le nostre conoscenze con leader del settore e decisori politici, vogliamo aiutare le organizzazioni ad anticipare i rischi, proteggere le infrastrutture critiche e costruire un futuro digitale più sicuro per tutti”. Dolman Aradori, Head of Cybersecurity di Ntt Data Italia, ha dichiarato: "L’intelligenza artificiale sta trasformando profondamente il modo in cui concepiamo la sicurezza informatica, rendendola più predittiva, adattiva e resiliente. Tuttavia, la vera sfida non è solo sfruttare la potenza dell’automazione, ma farlo in modo sicuro, trasparente e consapevole. Come Ntt Data crediamo che nel bilanciamento tra tecnologia e responsabilità si costruisca la fiducia digitale: una sicurezza che protegge i dati, i modelli e, soprattutto, le persone”. Sujoy Banerjee, Regional Business Director, ManageEngine, ha detto: "ManageEngine partecipa attivamente a CyberTech Europe dal 2023. Questo prestigioso evento dedicato alla sicurezza informatica continua a rappresentare una piattaforma preziosa per presentare le innovazioni della nostra suite completa di oltre 60 prodotti IT, inclusi gli ultimi progressi nelle nostre soluzioni di sicurezza informatica. Con l'attenzione rivolta quest'anno all'AI e all'agentic AI, eravamo particolarmente interessati a esplorare come le tecnologie emergenti stiano plasmando il futuro della difesa informatica. Abbiamo apprezzato l'opportunità di interagire con i visitatori dello stand in conversazioni approfondite sulle tendenze della sicurezza informatica, sulla conformità normativa e sulle best practice”. “La partecipazione a Cybertech – ha detto Elena Accardi, Country Manager di Zscaler in Italia - è stata un’importante occasione di confronto con clienti, partner e rappresentanti delle istituzioni su temi che riguardano la cybersecurity e la trasformazione digitale del Paese. Zscaler continua a crescere in Italia, affiancando le aziende nel loro percorso verso un modello di sicurezza moderno e cloud-based. Il nostro approccio Zero Trust è la chiave per consentire alle imprese di innovare in modo sicuro, riducendo la complessità e migliorando l’agilità operativa. Eventi come Cybertech rappresentano un momento prezioso per condividere esperienze, approfondire le sfide del futuro e rafforzare il dialogo all’interno dell’ecosistema della cybersecurity”. Luca Nilo Livrieri, Sr. Director, Sales Engineering, CrowdStrike, ha dichiarato: "A Cybertech Europe, metteremo in evidenza come CrowdStrike stia guidando la cybersecurity nell'era dell'IA. Le organizzazioni di tutta Europa sono impegnate in una vera e propria corsa contro il tempo: difendersi da avversari che sfruttano l'intelligenza artificiale per accelerare e potenziare i loro attacchi. CrowdStrike garantisce un vantaggio ai difensori attraverso la difesa agentica e una trasformazione radicale del SOC. Il ruolo degli analisti si evolve da figure che gestiscono gli alert manualmente, a professionisti che orchestrano e supervisionano team di agenti intelligenti che operano in autonomia. Come pionieri dell'AI Detection and Response (AIDR), stiamo definendo il futuro della cybersecurity: proteggere ogni livello dell'IA aziendale e consentire alle organizzazioni di sfruttare appieno il potenziale dell'intelligenza artificiale in totale sicurezza”. “Cybertech Europe, ogni anno, rappresenta un’occasione di condivisione e confronto utile per guardare al futuro della cybersecurity. Secondo il Data Security Report 2025 di Fortinet, nell’ultimo anno i

budget destinati alla sicurezza dei dati sono cresciuti nel 72% delle organizzazioni. Tuttavia, il 41% delle aziende ha comunque subito perdite milionarie a causa di incidenti cyber interni. In questo scenario, il nostro Cybersecurity Skills Gap Report 2025 evidenzia la stretta relazione tra i data breach e la carenza di conoscenze di sicurezza informatica nelle imprese, che emerge come la principale causa delle violazioni. In un contesto di rischio in costante ascesa ed evoluzione, diviene fondamentale per le aziende puntare su soluzioni di cybersecurity integrate e investire nella costante formazione del personale. Parliamo di un tema chiave, non più rimandabile, ma che al contrario deve essere messo al centro dell'approccio alla sicurezza di tutte le organizzazioni. In questa direzione, assumono un valore sempre più strategico le collaborazioni pubblico-privato, come quelle strette da Fortinet con ACN e la Polizia Postale, ma anche con le università, volte a migliorare la capacità di risposta collettiva alle minacce e a diffondere nel Paese una cultura della cybersecurity capace di coinvolgere tutte e tutti", ha dichiarato Massimo Palermo, VP & Country Manager Italia e Malta di Fortinet. Riccardo Scalzi, Head of Offer Engineering S3K, ha dichiarato: "Le tecnologie di cybersecurity dual use, cioè quelle che possono essere impiegate sia per scopi civili che militari, stanno già modificando profondamente la natura della conflittualità tra Stati. L'integrazione è la parola chiave, ed il saper integrare è diventato per noi un punto cardine grazie al quale riusciamo ad affrontare problematiche e necessità sotto diversi punti di vista. Nello scenario odierno diventa quasi scontato dover parlare di tematiche afferenti ad AI, Simulazione e Blockchain ma molto spesso è difficile capire in che modo queste singole componenti possano essere integrate e fornire un vero valore aggiunto nel campo della Cybersecurity. Si può ad esempio parlare di AI come il "cervello" dell'ecosistema di sicurezza. l'AI non solo automatizza il rilevamento delle minacce (ad esempio, analizzando enormi volumi di dati per identificare anomalie), ma può anche essere usata per prevedere i comportamenti degli aggressori. La Simulazione (What-if Analysis) permette di testare le difese aziendali contro scenari di attacco ipotetici prima che si verifichino. Questo approccio proattivo aiuta a identificare le vulnerabilità e a ottimizzare i piani di risposta. La Blockchain può essere utilizzata per garantire l'integrità e la sicurezza dei dati".

(Prima Notizia 24) Lunedì 27 Ottobre 2025