

Tecno - *Roma, conclusa la nona edizione di Cybertech Europe: la sicurezza digitale esordisce nell'era dell'IA*

Roma - 14 ott 2026 (Prima Notizia 24) **Chiuso il vertice nella capitale tra sovranità dei dati, minacce informatiche ad alta velocità e regolamentazioni comunitarie. L'allarme di Campora (Leonardo): "Rischiosa l'assenza di fondi dedicati nel bilancio dell'Unione Europea".**

Si è conclusa presso il centro congressi "La Nuvola" di Roma la nona edizione di Cybertech Europe 2026, la rassegna internazionale dedicata alla sicurezza digitale, alla protezione delle infrastrutture strategiche e alle nuove tecnologie. Durante i lavori è emerso come il settore abbia definitivamente varcato la soglia dell'era dell'intelligenza artificiale, ponendo al centro del dibattito l'impiego dei sistemi autonomi e il tema della sovranità dei dati. "Il futuro della cybersicurezza, che in realtà è anche un presente, sarà una sorta di competizione tra sistemi intelligenti, in cui l’essere umano ci sarà ancora ma come supervisore responsabile. Il nuovo gioco è un gioco alla velocità delle macchine e la cooperazione non è un’opzione", ha dichiarato Andrea Campora, dirigente della divisione Cyber & Security Solutions di Leonardo. Nel suo intervento in sessione plenaria, il manager ha evidenziato come la "mancanza di sovranità può diventare una vera vulnerabilità strategica" in un contesto di "resilienza sistemica". Riferendosi alle proposte per il nuovo quadro finanziario della Commissione europea, il rappresentante del gruppo ha espresso forte preoccupazione per la cornice contabile: "Nella proposta attuale, a differenza della precedente, non c’è un budget dedicato alla cybersicurezza. La settimana scorsa, in qualità di presidente di Ecso, ho firmato una lettera aperta alla Dg Grow per condividere i rischi di un simile approccio, che sottovaluta o non protegge a sufficienza ciò che è un investimento sulle fondamenta della nostra società". Contestazioni sono state mosse anche sul testo normativo per lo sviluppo informatico dell'Unione, che a suo avviso "impone una forte protezione cyber senza dire nulla su da dove debbano provenire le soluzioni di cybersicurezza", determinando la contraddizione per cui "si ha la certezza della proprietà europea dei dati, ma si delega altrove la capacità di proteggerli". Sul versante delle normative comunitarie si è espresso anche Marco Lucchina, responsabile per l'Italia della società di sicurezza Cynet, evidenziando che nello scenario odierno, segnato dal confronto tra Stati Uniti e Cina, "il fatto di avere un regolamento abbastanza restrittivo ci protegge, perché altrimenti ci sarebbe un’adozione indiscriminata e senza controllo" delle tecnologie digitali, aggiungendo che l'azienda ha "investito tanto nella compliance, certificazioni Acn, Ai Act, Cyber Resilience Act, oltre al Gdpr e a tutto quello che ne consegue nella varia regolamentazione", per "essere il più vicini possibili ai clienti, ai partner e alle pubbliche amministrazioni". Sull'evoluzione operativa degli attacchi informatici è intervenuto Umberto Pirovano, responsabile tecnico di Palo Alto Networks: "La cybersecurity ha varcato una soglia fondamentale, entrando a

pieno titolo nell'era dell'Ia. Il dibattito centrale si è concentrato su come l'Ia stia passando dall'essere un semplice strumento di supporto a un motore attivo e autonomo sia delle offensive sia delle difese informatiche. Ciò che è emerso chiaramente è che le organizzazioni si trovano a fare i conti con una profonda asimmetria. Gli attaccanti utilizzano strumenti di Frontier Ai per comprimere i cicli d'attacco di quasi il 97 per cento, eseguendo catene di compromissione complesse in ore o minuti, anziché in settimane". Nel prospettare i futuri assetti aziendali, il tecnico ha aggiunto: "Guardando al prossimo anno, la sfida principale per le aziende sarà gestire la rapida adozione di agenti di Ia autonomi, che agiscono a tutti gli effetti come una nuova classe di insider privileged, superando al contempo la grave frammentazione dovuta alle soluzioni puntuali e a un debito infrastrutturale globale nella cybersecurity stimato in 1.000 miliardi di dollari". Per affrontare questa transizione, per Pirovano le aziende "devono consolidare il proprio stack di sicurezza per eliminare i punti ciechi nella visibilità, applicare a ogni identità non umana di Ia rigidi controlli Zero Trust e schierare difese continue a velocità macchina per intercettare le minacce guidate dall'Ia prima che possano causare danni". A tale scopo, "il Ciso e il Cio devono agire in totale sintonia, spostando il proprio focus dalla semplice compliance alla velocità operativa e alla semplificazione architetturale. Poiché gli attacchi moderni supportati dall'intelligenza artificiale attraversano contemporaneamente reti, ambienti cloud, endpoint e identità, uno stack frammentato genera tempi di risposta ritardati che si rivelano fatali quando gli attacchi progrediscono in pochi minuti", rendendo indispensabile che "il Ciso e il Cio stabiliscano limiti e una governance rigida per l'adozione dell'Ia". Sull'affidabilità e la trasparenza degli strumenti avanzati si è soffermato Edoardo Accenti, direttore reti aziendali di Hpe Italia, rimarcando l'importanza che le imprese "possano avere il controllo, la visibilità e la trasparenza di quelli che sono gli algoritmi che stanno dietro all'intelligenza artificiale", al fine di "garantire un'Ia affidabile", cogliendo le opportunità di mercato e cercando di "raggiungere una maggiore competitività". Sull'integrazione dei programmi autonomi, Accenti ha evidenziato che si tratta di un'opportunità ma al contempo di una sfida, "perché estende quello che è il perimetro di sicurezza che dobbiamo andare poi a implementare", individuando le possibili soluzioni nell'adozione di architetture di rete e sistemi informatici dedicati. Sulle implicazioni di sicurezza interna per le aziende, Salvatore Frosina, co-amministratore delegato di Dgs, ha invitato a bilanciare la corsa all'innovazione con la responsabilità d'uso, definendo i sistemi operativi autonomi senza controllo "una bomba ad orologeria". "Oggi ogni dipendente sul proprio laptop potrebbe far funzionare un Agentic Ai, quindi chi si occupa della sicurezza delle organizzazioni deve essere sicuro che queste siano gestite, controllate. Devono lavorare in maniera corretta", ha avvertito il dirigente, evidenziando il rischio che l'impiego non autorizzato di strumenti personali possa "portare dati aziendali all'interno della rete". Di conseguenza, "dobbiamo utilizzarle ma saperlo fare con le tecnologie nostre, in modo tale da proteggere la sovranità nazionale, quindi con le nostre tecnologie, con le nostre attività". L'evento ha visto la partecipazione di esponenti delle istituzioni, delle aziende di settore e delle forze dell'ordine, tra i quali il ministro dell'Economia lituano Edvinas Griksas, l'amministratore delegato di Leonardo Lorenzo Mariani, il direttore della Polizia postale Ivano Gabrielli, l'amministratore delegato di Accenture Italia Teodoro Lio, l'amministratore delegato del Polo strategico nazionale Emanuele Iannetti e il presidente di Dgs Walter Ruffinoni. Nelle sessioni

precedenti, i vertici di Leonardo avevano ricordato come le minacce cibernetiche costituiscano "strumenti strategici capaci di minare la sicurezza nazionale, la stabilità economica e la fiducia dell’opinione pubblica", mentre la Polizia postale ha segnalato che in Italia circa l'80% delle vulnerabilità informatiche risulta legato ad errori di configurazione, gestione delle procedure o utilizzo improprio dei dispositivi da parte del personale, raccomandando maggiori investimenti nella formazione e nella cultura digitale dei giovani.

(Prima Notizia 24) Mercoledì 14 Ottobre 2026