

Cybersicurezza, Tito (Ibm): "Attacchi iniziati con applicazioni pubbliche aumentano del 44%"

Descrizione

(Adnkronos) "La crescente frequenza e sofisticazione degli attacchi informatici impone alle organizzazioni di ripensare radicalmente il proprio approccio alla sicurezza digitale. Nel report X-Force Threat Intelligence Index 2026, Ibm ha registrato un aumento del 44% degli attacchi iniziati con lo sfruttamento di applicazioni pubbliche, in gran parte causati dalla mancanza di controlli di autenticazione e dalla scoperta di vulnerabilità consentita dall'AI". Lo ha dichiarato Cristiano Tito, Cybersecurity Services Portfolio Lead Ibm Italia, in occasione della quinta edizione di Cybersec, la conferenza internazionale in corso a Roma e organizzata dal quotidiano Cybersecurity Italia.

Tito illustra poi le soluzioni per affrontare la situazione: "Per affrontare questa sfida la sicurezza deve evolvere su due fronti: AI per la sicurezza, che sfrutta l'intelligenza artificiale per automatizzare compiti, analizzare minacce e generare risposte, e sicurezza per l'AI, volta a proteggere modelli, dati e flussi di lavoro da attacchi sofisticati, come prompt malevoli o deep fake. È necessario quindi un framework strutturato basato su principi zero trust e tecnologie emergenti come firewall AI e Mldr (Machine Learning Detection and Response)".

All'orizzonte si profila poi un'altra sfida: il Quantum Computing. Questa tecnologia promette potenza di calcolo senza precedenti, ma rischia di rendere obsoleti gli algoritmi crittografici tradizionali, esponendo dati sensibili ad attacchi harvest now, decrypt later. L'Unione Europea ha suggerito un piano per la transizione alla Crittografia Post-Quantistica (Pqc) entro il 2035, sottolineando l'importanza di un passaggio tempestivo, completo e coordinato. È chiaro che il futuro della cybersecurity sarà ibrido, dominato da due forze trasformative: AI e Quantum Computing. Minacce e opportunità si intrecciano in una corsa globale dove chi saprà integrare queste tecnologie come alleate avrà un vantaggio strategico decisivo, non solo nella protezione dei dati ma nella leadership geopolitica e tecnologica".

"

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione

Marzo 4, 2026

Autore

redazione

default watermark