Capgemini press contacts:
Tiziana Sforza
Marketing & Communication
tiziana.sforza@capgemini.com
+39 348 7018984

L'AI e la Gen AI sono destinate a trasformare la cybersecurity per la maggior parte delle organizzazioni

Se da un lato la Gen AI aumenta le vulnerabilità, dall'altro più della metà delle organizzazioni ritiene che l'uso di questa tecnologia possa accelerare il rilevamento delle minacce e migliorarne l'accuratezza

Milano, 12 dicembre 2024 – Il nuovo report del Capgemini Research Institute, "*New defenses, new threats: What AI and Gen AI bring to cybersecurity*", suggerisce che sebbene stiano emergendo nuovi rischi in materia di cybersecurity, derivanti dalla proliferazione dell'AI e dell'AI generativa (Gen AI), queste tecnologie rappresentano un cambiamento trasformativo nel rafforzamento delle strategie di cyber-difesa a lungo termine che consentono di anticipare, rilevare e rispondere alle minacce. Due terzi delle organizzazioni considerano ormai prioritaria l'AI nelle loro operazioni di sicurezza.

Secondo il report, se da un lato l'AI è considerata dalle organizzazioni una tecnologia strategica per il rafforzamento delle proprie strategie di sicurezza, dall'altro la crescente adozione della Gen AI in vari settori[1] comporta una maggiore vulnerabilità. L'intelligenza artificiale generativa introduce tre principali aree di rischio per le organizzazioni: attacchi più sofisticati con un maggior numero di avversari, l'espansione della superficie di attacco informatico e l'aumento delle vulnerabilità nell'intero ciclo di vita delle soluzioni personalizzate di Gen AI. Questi rischi sono inoltre aggravati dall'uso improprio dell'AI e dell'AI generativa da parte dei dipendenti, con un conseguente aumento significativo del rischio di violazioni dei dati.

Due organizzazioni su tre temono una maggiore esposizione alle minacce
Quasi tutte le organizzazioni intervistate (97%) affermano di aver riscontrato violazioni o problemi di sicurezza legati all'uso della Gen AI nell'ultimo anno. Questa tecnologia comporta anche rischi aggiuntivi, tra cui allucinazioni, generazione di contenuti distorti, dannosi o inappropriati e attacchi di tipo *prompt injection*[2]. Due organizzazioni su tre (67%) sono preoccupate per l'inquinamento dei dati e per la possibile fuga di dati sensibili attraverso i dataset utilizzati per l'addestramento dei modelli di intelligenza artificiale generativa.

Inoltre, la capacità della Gen AI di generare contenuti sintetici altamente realistici sta comportando ulteriori rischi: oltre due aziende intervistate su cinque (43%) hanno dichiarato di aver subito perdite finanziarie derivanti dall'uso di *deepfake*.

Circa 6 organizzazioni su 10 ritengono inoltre di dover aumentare il budget destinato alla cybersecurity per rafforzare adeguatamente le proprie difese.

[1] Quasi un quarto (24%) delle organizzazioni intervistate ha abilitato le funzionalità di Gen AI in alcune o nella maggior parte delle proprie funzioni e sedi (Capgemini Research Institute, *"Harnessing the value of generative AI 2nd edition: Top use cases across sectors"*, luglio 2024).
[2] Gli attacchi di tipo *prompt injection* comportano l'utilizzo di input dannosi per manipolare i modelli di AI e di Gen AI, compromettendone l'integrità.

L'AI e la Gen AI sono fondamentali per rilevare e rispondere agli attacchi
L'indagine, condotta su 1.000 organizzazioni[3] interessate all'utilizzo dell'AI nell'ambito della cybersecurity o che già la stanno utilizzando, rileva che la maggior parte di esse si affida a questa tecnologia per rafforzare la sicurezza dei dati, delle applicazioni e del cloud, grazie alla sua capacità di analizzare rapidamente grandi quantità di dati, identificare modelli di attacco e prevedere potenziali violazioni.

Oltre il 60% delle aziende intervistate ha registrato una riduzione di almeno il 5% del proprio *time-to-detect*, mentre quasi il 40% ha dichiarato che il tempo di ripristino è diminuito almeno del 5% a seguito dell'implementazione dell'AI nei propri centri operativi di sicurezza (SOC).

Tra le organizzazioni intervistate, tre su cinque (61%) ritengono che l'AI sia essenziale per una risposta efficace alle minacce, in quanto consente loro di implementare strategie di sicurezza proattive contro attori sempre più sofisticati. Inoltre, la stessa percentuale ritiene che l'intelligenza artificiale generativa sia in grado di rafforzare le strategie di difesa proattiva a lungo termine, grazie a un rilevamento più rapido delle minacce. Oltre la metà ritiene inoltre che questa tecnologia consentirà agli analisti di cybersecurity di concentrarsi maggiormente sulle strategie di contrasto a minacce più complesse.

"L'uso dell'AI e della Gen AI si è finora rivelato un'arma a doppio taglio. Se da un lato introduce rischi senza precedenti, dall'altro le organizzazioni si stanno affidando sempre più all'AI per un rilevamento più rapido e accurato degli incidenti informatici. L'AI e l'AI generativa forniscono ai team di sicurezza nuovi e potenti strumenti per limitare questi incidenti e trasformare le loro strategie di difesa. Per garantire che rappresentino un vantaggio significativo di fronte a minacce sempre più sofisticate, le organizzazioni devono mantenere e dare priorità al monitoraggio continuo dell'evoluzione delle minacce informatiche, costruire in modo adeguato l'infrastruttura di gestione dei dati, i framework per l'adozione dell'AI e le relative linee guida etiche e introdurre validi programmi di formazione e sensibilizzazione dei dipendenti", ha dichiarato **Monia Ferrari**, **Amministratore Delegato di Capgemini in Italia**.

Metodologia di ricerca
Il Capgemini Research Institute ha intervistato 1.000 organizzazioni interessate a considerare l'utilizzo dell'AI per la cybersecurity o che già la stanno utilizzando, in 12 settori e 13 paesi appartenenti alle regioni dell'Asia-Pacifico, dell'Europa e del Nord America. Queste organizzazioni hanno un fatturato annuo pari o superiore a 1 miliardo di dollari. L'indagine globale si è svolta nel maggio 2024. Le organizzazioni intervistate rappresentano una vasta gamma di settori, tra cui automotive, beni di consumo, retail, banche, assicurazioni, telecomunicazioni, energia e utility, aerospaziale e difesa, high-tech, produzione di apparecchiature industriali, farmaceutica e sanità e settore pubblico.

Capgemini
Capgemini, partner globale per la trasformazione tecnologica e di business delle aziende, supporta i suoi clienti nella loro transizione verso un mondo più digitale e sostenibile, creando impatto positivo per le imprese e la società. Capgemini è un gruppo responsabile e diversificato di 340.000 persone presente in più di 50 paesi nel mondo. Oltre 55 anni di esperienza rendono Capgemini un partner affidabile per i suoi clienti, in grado di fornire soluzioni innovative per le loro esigenze di business. Capgemini offre servizi e soluzioni end-to-end, dalla strategia e progettazione all'ingegneria, grazie alle sue competenze all'avanguardia in ambito AI, cloud e dati, alla sua esperienza settoriale e al suo ecosistema di partner. Nel 2023 il Gruppo ha registrato ricavi complessivi pari a 22,5 miliardi di euro.

Get the Future You Want | www.capgemini.com

Capgemini Research Institute
Il Capgemini Research Institute è il think-tank interno di Capgemini dedicato a tutto ciò che è digitale. L'istituto pubblica lavori di ricerca in merito all'impatto delle tecnologie digitali sulle grandi aziende

[3] 1.000 organizzazioni in 12 settori e 13 paesi appartenenti alle regioni dell'Asia-Pacifico, dell'Europa e del Nord America, con un fatturato annuo pari o superiore a 1 miliardo di dollari.

tradizionali. Il team fa leva sul network mondiale di esperti Capgemini e lavora a stretto contatto con partner accademici e tecnologici. L'istituto possiede centri di ricerca dedicati in India, Singapore, nel Regno Unito e negli Stati Uniti. Recentemente, è stato nominato il miglior istituto di ricerca al mondo per la qualità dei suoi lavori da una giuria di analisti indipendenti.

Per saperne di più consultare il sito https://www.capgemini.com/it-it/capgemini-research-institute/