Come l'IA ridefinirà il settore della cybersecurity

A cura di Yves Kramer, Senior Investment Manager di Pictet Asset Management

06.12.2023

- ***Gli attacchi informatici rappresentano oggi una grave minaccia: si stima che ogni giorno vengano sottratti in modo illecito 3,8 milioni di dati. L'AI rappresenta in tal senso una sfida e un'opportunità per la cybersecurity.***
- ***Oggi esistono circa 15 miliardi di dispositivi interconnessi al mondo e secondo le previsioni il loro numero raddoppierà nell'arco di 10 anni. Ognuno di essi dovrà essere protetto.***
- ***In questo contesto, il settore della cybersecurity rappresenta un'opportunità di investimento interessante, poiché destinato a crescere sempre di più.***

Se ricevessimo un messaggio di posta elettronica scritto male, nel quale ci venga offerta una quota di una misteriosa un'eredità, sentiremmo subito puzza di bruciato. Ma reagiremmo allo stesso modo se si trattasse di una mail dall'aspetto autentico proveniente dal tuo ufficio Risorse Umane o di un messaggio vocale implorante di tuo figlio? Con l'aiuto dell'intelligenza artificiale (IA) gli attacchi informatici diventeranno sempre più sofisticati e difficili da individuare: questo rappresenta una grande sfida per il settore della cybersecurity, ma costituisce anche una grossa opportunità per le aziende di sicurezza in grado di sfruttare le potenzialità dell'IA.

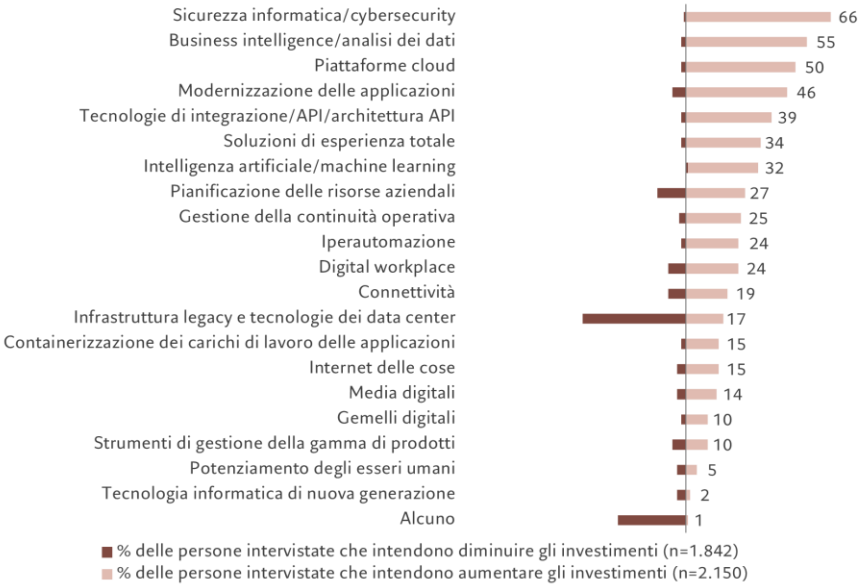
Gli attacchi informatici rappresentano già oggi una grave minaccia: ogni 39 secondi si verifica un'infiltrazione di hacker, e si stima che ogni giorno vengano sottratti in modo illecito 3,8 milioni di dati[1]. Non sorprende, quindi, che secondo Gartner il settore della cybersecurity sia destinato a crescere di quasi il 14% quest'anno; tuttavia, vista la sempre maggiore diffusione dell'IA, riteniamo che in futuro la sua crescita potrebbe risultare ancora più rapida. Poiché è in grado di aumentare la portata e la gravità degli attacchi, l'IA darà sicuramente un impulso maggiore agli investimenti nella cybersecurity in un'ampia gamma di settori. I modelli linguistici di grandi dimensioni (LLM) che alimentano le nuove forme di IA stanno semplificando notevolmente la programmazione, il che, a sua volta, significa che sarà più facile produrre malware e diffonderli. Infatti, un aspirante hacker, anche se privo di competenze tecnologiche specialistiche, grazie all'IA sarà in grado di ottenere informazioni su precedenti violazioni, che potrà sfruttare per attuare attacchi simili, potenzialmente su più siti contemporaneamente. Le e-mail di spear phishing ben mirate e altamente personalizzate che distribuiscono e installano malware stanno già iniziando a sostituire i maldestri testi generici e i formati PDF.

L'IA generativa amplia, quindi, la portata della disinformazione, e consente agli hacker di vagliare senza alcuna difficoltà le informazioni ottenute e colmare eventuali lacune nei dati. Inoltre, gli hacker potranno anche riuscire a manipolare a proprio vantaggio i modelli di IA delle loro vittime, coprendo le proprie tracce o persino perpetrando gli attacchi. Ciò potrebbe danneggiare non solo gli individui, ma anche aziende e governi. Le implicazioni vanno oltre i meri dati: l'aumento dell'uso di veicoli a guida autonoma o semi-autonoma potrebbe, ad esempio, compromettere la sicurezza dei trasporti.
E i rischi dell'IA non si limitano agli attacchi attivi. I dirigenti aziendali sono preoccupati anche per la conformità alle normative sulla privacy dei dati e per le implicazioni dei contenuti creati dall'IA riguardo la proprietà intellettuale; per questo motivo stanno dando priorità agli investimenti in

[1] https://ung.edu/continuing-education/news-and-media/cybersecurity.php

soluzioni di sicurezza dei dati e di governance[2]. Secondo Gartner, due terzi delle aziende stanno pianificando di aumentare il budget destinato alla sicurezza informatica rispetto al 2022 spinti dalla paura di subire perdite finanziarie[3].

Fig.1 - L'investimento in tecnologie di sicurezza rimane una priorità per le aziende
% di aziende intervistate che intendono aumentare/diminuire gli investimenti in sicurezza tecnologica nel 2023 rispetto al 2022



Fonte: Sondaggio CIO e Technology Executive di Gartner 2023

In questo scenario risiede un'opportunità, sia per il settore della sicurezza sia per gli investitori: le aziende di cybersecurity in grado di adottare l'IA per mettere in atto soluzioni di difesa digitale avranno solide prospettive di crescita nei prossimi anni. Questo vale soprattutto per coloro che privilegiano investimenti in infrastrutture, come il caso di Equinix. Questa azienda è consapevole che la proliferazione dei dispositivi interconnessi e il crescente utilizzo dell'IA stanno creando un numero sempre maggiore di dati che devono essere archiviati e trasferiti in modo sicuro, il che a propria volta richiede un'infrastruttura affidabile. Equinix utilizza il machine learning per migliorare la sicurezza dei propri data center, individuando ed eliminando eventuali punti deboli. Ciò può includere l'uso di macchine per analizzare le videoriprese alla ricerca di qualsiasi attività sospetta all'interno o intorno al data center, oltre che il monitoraggio dell'accesso ai propri dati da parte di clienti per segnalare eventuali anomalie[4].

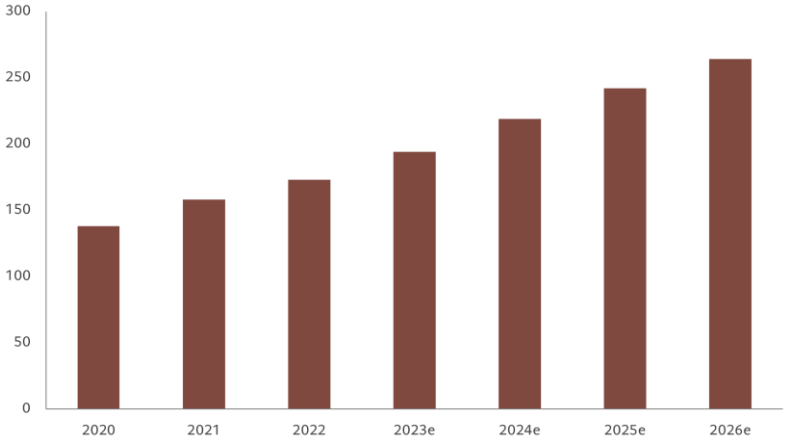
Le aziende possono anche puntare sullo sviluppo di servizi e software specializzati per ottenere un vantaggio competitivo nel settore della cybersecurity sempre più dominato dall'IA. Questa strategia è già stata adottata da aziende come la statunitense Crowdstrike, che sta sfruttando la sua vasta cronologia di dati e telemetrie per dotare i nuovi moduli di funzionalità di IA sulla sua piattaforma Falcon. Particolarmente diffuso tra le grandi aziende statunitensi, Falcon è progettato per rilevare tempestivamente le minacce informatiche sui computer di un'azienda.
Analogamente, Palo Alto Networks, il più grande fornitore autonomo di cybersecurity, offre oggi una gamma di soluzioni incentrate su cloud e IA. Inoltre, è in crescita il mercato dei software sicuri da utilizzare in veicoli a guida autonoma per garantire la sicurezza dei trasporti.

[2] https://business.bofa.com/content/dam/flagship/bank-of-america-institute/transformation/cybersecurity-landscape-impact-what-comes-next.pdf
[3] Sondaggio CIO e Technology Executive di Gartner 2023
[4] https://blog.equinix.com/blog/2022/09/14/6-reasons-why-you-need-ai-ml-in-your-data-center/

L'IA potrebbe anche far sorgere nuovi sottosettori nell'industria della cybersecurity: ad esempio, la creazione di un nuovo mercato per il controllo delle informazioni generate da sistemi di IA. Inoltre, saranno necessarie nuove metodologie per verificare l'identità umana e questo potrebbe aprire le porte a nuove start-up, generando ulteriori opportunità di crescita per le aziende di cybersecurity già esistenti. La sfida per le aziende che operano nel settore della sicurezza è creare una nuova generazione di strumenti di cybersecurity che integrino l'IA generativa per individuare la presenza di malware velocemente e su vasta scala. La maggior dipendenza dall'IA come supporto all'offerta di servizi di cybersecurity acquisirà maggiore importanza, data la carenza di competenze nel settore.

Fig.2 - Spesa in soluzioni per la sicurezza, una tendenza strutturale

Spesa mondiale in soluzioni per la sicurezza, in miliardi di dollari



Fonte: Gartner, Forecast Analysis Information Security and Risk Management Worldwide

Anche nelle aziende di cybersecurity sta crescendo l'importanza dell'IA, per via di un mutamento delle priorità commerciali. Negli ultimi anni, il settore è andato incontro a notevoli cambiamenti che hanno visto le aziende concentrarsi meno sui prodotti che proteggono gli endpoint (desktop, laptop e dispositivi mobili) e più su quelli che proteggono l'insieme delle reti aziendali e che operano nel cloud. Proprio in queste ultime, infatti, l'IA presenta maggiori rischi di cybersecurity. Per questo motivo le aziende stanno sviluppando soluzioni zero trust che verificano continuamente le credenziali degli individui che interagiscono con un'organizzazione, sia internamente che esternamente.

Nel complesso, i progressi compiuti nell'IA e nel machine learning rappresentano tendenze a lungo termine che incrementeranno la domanda di servizi di cybersecurity da parte di governi, aziende e singoli individui. Poiché le soluzioni di sicurezza basate sull'IA offrono una maggiore automazione, ad esempio nel caso delle attività ripetitive svolte dal dipartimento di analisi nei centri operativi per la sicurezza, è ipotizzabile che le spese per i software di sicurezza aumenteranno. Questo dovrebbe, a propria volta, contribuire ad alleviare la carenza di personale qualificato nel campo della cybersecurity, che attualmente ammonta a 3,4 milioni di persone[5].
Tutto ciò rafforzerà ulteriormente il potenziale di crescita del settore: oggi esistono circa 15 miliardi di dispositivi interconnessi al mondo e, secondo le previsioni, il loro numero raddoppierà nell'arco di 10 anni e ognuno di essi dovrà essere protetto[6]. Le aziende di cybersecurity che utilizzano i più recenti progressi tecnologici a proprio vantaggio saranno probabilmente quelle che ne beneficeranno maggiormente.

[5] https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196
[6] https://transformainsights.com/research/forecast/highlights

Il Gruppo Pictet

Fondato a Ginevra nel 1805, il Gruppo Pictet è uno dei principali gestori patrimoniali e del risparmio indipendenti in Europa. Con un patrimonio gestito e amministrato che ammonta a circa 653 miliardi di euro al 30 giugno 2023, il Gruppo è controllato e gestito da otto soci e mantiene gli stessi principi di titolarità e successione in essere fin dalla fondazione. Il Gruppo Pictet, con oltre 5.300 dipendenti, ha il suo quartier generale a Ginevra e altre sedi nei seguenti centri finanziari: Amsterdam, Barcellona, Basilea, Bruxelles, Dubai, Francoforte, Hong Kong, Londra, Losanna, Lussemburgo, Madrid, Milano, Montreal, Monaco di Baviera, Nassau, New York, Osaka, Parigi, Principato di Monaco, Roma, Shanghai, Singapore, Stoccarda, Taipei, Tel Aviv, Tokyo, Torino, Verona e Zurigo. Pictet Asset Management ("Pictet AM") comprende tutte le controllate e le divisioni del Gruppo Pictet che svolgono attività di asset management e gestione fondi istituzionali. Fra i principali clienti si annoverano alcuni dei maggiori fondi pensione, fondi sovrani e istituti finanziari a livello mondiale.

Contatti Stampa:
BC Communication
Lucrezia Pisani | Tel. +39 347 6732479 | lucrezia.pisani@bc-communication.it
Carla Parisi | Tel. +39 339 5796751 | carla.parisi@bc-communication.it