Intelligenza Artificiale & Cybersecurity

L'inizio di una nuova era

it.allianzgi.com

Ad uso esclusivo e riservato ai distributori di fondi ed investitori professionali.

Punti chiave

- Nel quadro della crescente digitalizzazione della vita quotidiana la cybersecurity assume un'importanza strategica per la protezione di dati e asset.
- L'intelligenza artificiale (AI) può rappresentare la giusta soluzione per fronteggiare alcuni dei rischi informatici più insidiosi in un contesto sfidante in rapida evoluzione.
- Con l'introduzione di nuove leggi da parte di autorità e governi, la spesa aziendale per la cybersecurity diverrà probabilmente una priorità.

La nuova era della cybersecurity

Per cybersecurity si intendono le pratiche volte a proteggere computer, dispositivi mobili e altri asset digitali da attacchi dolosi. Negli ultimi decenni i cyberattacchi sono diventati un pericolo sempre più concreto per aziende e singoli individui. L'ascesa della tecnologia ha comportato una maggiore interconnessione tra i sistemi delle organizzazioni e un incremento della presenza online dei singoli. I cybercriminali sfruttano tale evoluzione che accresce le opportunità di accedere a dati sensibili e distruggerli. Pertanto una cybersecurity efficace è ormai essenziale per società di qualsiasi tipo e dimensione[1].

COVID-19 e impatti sulla cybersecurity

La pandemia ha messo in luce quanto impreparate fossero le organizzazioni ad affrontare la questione della cybersecurity. Il passaggio al lavoro da remoto e il crescente ricorso ai canali digitali hanno determinato un aumento delle problematiche in materia di cybersecurity. In molti casi organizzazioni e singoli individui faticano ad aggiornare i sistemi e a proteggere i dati. Alla luce di minacce sempre più frequenti è fondamentale eseguire costanti controlli di sicurezza e test di vulnerabilità. Molto spesso le società si avvalgono dell'AI per gestire i sempre più numerosi vettori di minacce utilizzati per i cyberattacchi. Anche per i team di sicurezza informatica delle grandi società è quasi impossibile monitorare tutte le minacce e passare in rassegna centinaia di migliaia di possibili vulnerabilità[2]. Di conseguenza, per allontanare le minacce informatiche si è deciso di ricorrere attivamente all'automazione mediante l'intelligenza artificiale (AI) e l'uso di algoritmi di apprendimento automatico. La pandemia ha innescato un cambio di approccio alla cybersecurity e le società ben posizionate, in grado di contribuire alla risoluzione delle problematiche più pressanti in materia, dovrebbero registrare una crescita consistente.

I danni causati dal cybercrimine potrebbero ammontare a US$6.000 miliardi annui nel 2021, il doppio rispetto ai US$3.000 miliardi del 2015.

Il costo elevato del cybercrimine

I costi del cybercrimine si riferiscono a danneggiamento o distruzione di dati, sottrazione di denaro, furto di proprietà intellettuale, sottrazione di dati personali e finanziari, appropriazione indebita, frode e danno reputazionale, e altro ancora. I danni causati dal cybercrimine potrebbero ammontare a US$6.000 miliardi annui nel 2021, il doppio rispetto ai US$3.000 miliardi del 2015. Si tratta del maggior trasferimento di capitali nella storia potrebbe essere più redditizio del traffico delle principali sostanze stupefacenti illegali a livello globale[3].

Il contributo dell'AI alla cybersecurity

Le società di tutto il mondo sono impegnate nella ricerca di soluzioni per combattere e ridurre il cybercrimine. L'AI si sta rivelando la tecnologia migliore e più adatta a risolvere alcuni dei principali problemi nell'area della cybersecurity. Il ricorso all'intelligenza artificiale e al Machine Learning per automatizzare l'individuazione delle minacce consente di rispondere in maniera più efficace agli attacchi informatici di quanto non avvenga con i tradizionali approcci basati su software.

Prima del 2019 appena il 20% circa dei provider di soluzioni di cybersecurity utilizzava l'AI. A fine 2020 tale percentuale dovrebbe attestarsi al 63%[4].

L'automazione permette alle società di distinguere fra condotte "virtuose" e "criminali" tramite modelli predittivi e dati passati. Tali modelli sono abbastanza intelligenti da individuare e prevenire in tempo reale numerose minacce informatiche. Eliminando la necessità dell'intervento umano gli ingegneri di cybersecurity possono concentrarsi su altri aspetti della protezione che potrebbero richiedere maggiore attenzione. L'AI può inoltre utilizzare i dati sui cyberattacchi di più aree e settori a livello globale per migliorare costantemente l'efficacia e i tassi di rilevamento. Di seguito sono riportati alcuni esempi dell'utilizzo dell'AI per la cybersecurity[5]:

Anti-spam: L'apprendimento automatico consente di sviluppare filtri più intelligenti per il rilevamento automatico e l'analisi di e-mail spam.

Biometrica: Le tecniche di autenticazione come le impronte digitali e la scansione facciale o dell'iride sono sempre più utilizzate in ambito lavorativo e domestico. L'AI contribuisce ad accrescere l'accuratezza del riconoscimento e fornisce indicazioni comportamentali per migliorare la sicurezza.

Rilevazione delle possibili minacce: Il riconoscimento avanzato dei pattern permette la rilevazione di minacce e virus in tempo reale così da rafforzare i sistemi di difesa e consentire una risposta più rapida e puntuale.

Elaborazione del linguaggio: L'AI può ricavare informazioni da articoli o ricerche per apprendere le ultime novità in materia di sicurezza informatica, tecniche di hackeraggio e strategie di prevenzione.

Rilevazione di bot (processo automatizzato inteso a simulare il comportamento di un essere umano – ad esempio navigare, riempire form, interagire): I modelli di apprendimento profondo (deep learning) sono in grado di apprendere il comportamento degli utenti e stabilire se determinate azioni siano anomale. Tali modelli consentono di individuare rapidamente i bot, distinguere i falsi account da quelli appartenenti a persone in carne e ossa e ridurre al minimo le minacce e i rischi.

Zero Trust: Questo modello di cybersecurity presuppone che le minacce provengano tanto dall'esterno quanto dall'interno della rete aziendale. AI e apprendimento automatico permettono il monitoraggio in tempo reale di log-in, location, dispositivi e indirizzi IP degli utenti, nonché il ricorso ad applicazioni provenienti solo da fonti affidabili.

Cybercrimine e Internet of Things (IoT)

Un dispositivo IoT (Internet of Things) è un hardware che trasmette dati da un punto a un altro mediante Internet. Nel 2018 i dispositivi IoT sono stati i principali strumenti utilizzati per commettere reati in ambito tecnologico. Nel 2019 i cyberattacchi tramite dispositivi IoT sono aumentati del 300% per via della proliferazione di device digitali di uso quotidiano[6]. Tale impennata si deve in particolare a dispositivi IoT vulnerabili a causa di firmware obsoleti e mai aggiornati.

Gran parte dei dispositivi IoT è stata realizzata tenendo conto solo della funzionalità. Hanno sistemi operativi molto basilari e in genere la sicurezza è considerata un componente aggiuntivo.

Cisco stima che nel 2023 i dispositivi IoT saranno tre volte più numerosi della popolazione globale[7].

Ecco perché in passato i dispositivi IoT erano molto esposti alle minacce informatiche. Oggi anche in ambito IoT si adottano nuovi standard di cybersecurity per una migliore protezione dei dispositivi smart. Un altro trend che sottolinea l'importanza della cybersecurity è la rapida adozione di soluzioni in cloud. Nel 2021 il volume complessivo di dati archiviati nel cloud – che comprende cloud pubblici gestiti da vendor e società di social media, cloud governativi e cloud privati – sarà 100 volte superiore a quello del 2019[8]. Le società avranno quindi bisogno di soluzioni di sicurezza più sofisticate.

Governi, autorità internazionali e nuove leggi

La legislazione, ad esempio il Regolamento generale per la protezione dei dati (GDPR) dell'Unione Europea (UE), sostiene la spesa aziendale per la cybersecurity. Ai sensi del GDPR le società che raccolgono dati sui cittadini dell'UE devono conformarsi a rigidi requisiti per la protezione dei dati dei clienti anche se non hanno una presenza commerciale nell'area[9]. La non conformità alle disposizioni può comportare pesanti multe, sino al 4% dei ricavi globali della società. È probabile che altri Paesi seguano l'esempio dell'UE e adottino regole e standard analoghi. Negli Stati Uniti la National Association of Corporate Directors ha invitato i consigli di amministrazione delle aziende ad accrescere le competenze e la governance in materia di cybersecurity[10]. Tutti i CdA dovrebbero essere in grado di comprendere e gestire le problematiche legate alla cybersecurity. Anche gli azionisti hanno aspettative simili: nel 2018 il 36% delle proposte avanzate dall'azionariato riguardava l'introduzione di parametri per la misurazione della performance ambientale e sociale, anche in termini di cybersecurity e privacy, ai fini della determinazione del compenso dei dirigenti. Inoltre, attualmente il Congresso USA sta esaminando il "Cybersecurity Disclosure Act of 2019"; se la legge sarà approvata le società quotate dovranno acquisire competenze in tema di cybersecurity oppure il CdA dovrà dimostrare alla Securities & Exchange Commission che tali competenze non sono necessarie[11]. Le organizzazioni non possono più rimandare gli interventi di cybersicurezza e l'AI si è dimostrata la tecnologia disponibile più pratica ed efficace in quest'area.

La cybersecurity e la rivoluzione dell'AI

Da sempre la sicurezza è fondamentale per la collettività. Nel quadro della transizione a un mondo più digitalizzato, cambiano le modalità di attuazione delle misure di sicurezza e numerose aziende propongono soluzioni innovative per contribuire a combattere i pericoli. CrowdStrike* è una società leader nella cybersecurity che fornisce servizi di ultima generazione per la endpoint security, la cyber threat intelligence e la pronta reazione ad eventuali incidenti informatici. CrowdStrike offre una piattaforma cloud che raccoglie dati sui cyberattacchi e sfrutta l'AI per migliorare costantemente il profilo di sicurezza dei dispositivi dei clienti. Splunk* sviluppa un software che consente alle aziende di cercare, correlare, analizzare, monitorare e comunicare dati in tempo reale. La tecnologia di Splunk potrebbe rivelarsi fondamentale per facilitare l'assimilazione e l'analisi di consistenti volumi di dati strutturati e non sulla cybersecurity da parte dei sistemi di AI. Okta* è un provider di software di cybersecurity pensati per impedire i furti di identità grazie a soluzioni di autenticazione e identificazione basate su rischi che fanno ricorso ad apprendimento automatico e AI per raccogliere informazioni sul comportamento contestuale.

Conclusioni

Sotto molti punti di vista l'AI era già utilizzata per migliorare la cybersecurity e combattere il cybercrimine. Oggi, con l'ascesa della tecnologia e il passaggio ai canali digitali, il ruolo dell'AI è più importante che mai. L'automazione e la rilevazione in tempo reale sono essenziali poiché sono gli strumenti più efficaci a disposizione delle società per difendersi dal costante aumento dei rischi informatici. In futuro la maggior parte dei settori e delle aziende di tutte le dimensioni avrà bisogno di strumenti di cybersecurity efficaci. Crediamo pertanto che gli investitori lungimiranti saranno ricompensati per aver selezionato attivamente società destinate a contribuire alla lotta al cybercrimine.

Allianz Global Artificial Intelligence

L'intelligenza artificiale trasforma il nostro modo di vivere e i settori dell'economia da anni, eppure siamo appena agli inizi di una rivoluzione che creerà numerose opportunità. A differenza dei fondi tecnologici già disponibili, Allianz Global Artificial Intelligence coglie il potenziale dirompente delle tecnologie di intelligenza artificiale, ne analizza le prospettive catturandone la crescita dinamica e sostenibile trasversale su tutti i mercati.

La strategia investe lungo tutta la catena del valore: dalle società tecnologiche che sviluppano l'infrastruttura e consentono l'applicazione dell'AI alle aziende attive in differenti settori che si avvalgono dell'AI per i loro prodotti, le loro soluzioni e i processi aziendali. L'intelligenza artificiale trasformerà profondamente ogni settore e di conseguenza chi disporrà delle competenze e delle capacità adeguate potrà beneficiare di innumerevoli opportunità di investimento diversificate. Allianz Global Artificial Intelligence offre agli investitori un'esposizione azionaria globale e diversificata al tema dell'intelligenza artificiale, senza vincoli di capitalizzazione, con focus sulle sulle mid e large cap. Il team di gestione del portafoglio, che ha sede a San Francisco, conta decenni di esperienza nella ricerca di società innovative e ha instaurato importanti relazioni nella Silicon Valley sia con società note al grande pubblico sia con innovative start up, vantaggi che consentono di stare al passo con la rapida evoluzione dell'AI. La piattaforma proprietaria AllianzGI Global Research offre una prospettiva globale e trasversale. Grazie alla comprensione delle tecnologie e delle aziende sottostanti, il nostro team gode di una posizione ottimale per poter capire le opportunità presentate dall'intelligenza artificiale in tutte le aree dell'economia globale.

1 La rivoluzione dell'AI è appena iniziata

- L'AI si sta evolvendo rapidamente e **non sarà solo una meteora**.
- Gli investimenti globali nelle start up basate sull'AI si sono **decuplicati** rispetto al 2012[12].
- L'AI sta trasformando i **business model** e i tradizionali modus operandi.
- L'AI è in grado di **accelerare l'apprendimento** e la produttività dell'uomo.
- Entro il 2030[13] l'AI potrebbe apportare all'economia globale **USD 15.700 miliardi**.

2 Opportunità di crescita a lungo termine

- Indipendentemente dal clima
- economico, i Paesi riconoscono che la **crescita futura è legata agli investimenti dell'innovazione.**
- L'AI si può considerare come uno **tsunami** che consentirà di modernizzare vari settori e trainare la crescita economica.
- Gli investitori che desiderano
- **incrementare i rendimenti** possono prendere parte alle opportunità di crescita di lungo periodo offerte dall'AI.
- L'AI come driver principale delle **reti 5G e della gestione delle risorse** genera interessanti opportunità di crescita.

3 Ampio universo di società innovative

- La nostra piattaforma di ricerca analizza oltre **1.000 società innovative.**
- Selezioniamo aziende **destinate a beneficiare di**:
  - Impiego di infrastrutture per l'AI;
  - Sviluppo di software e applicazioni basati sull'IA;
  - Adozione in settori legati all'AI.
- Il portafoglio è costruito per cogliere il potenziale della **prossima rivoluzione tecnologica** su scala globale in differenti settori e segmenti.

[1] Digital McKinsey and Global Risk Practice, "Cybersecurity in a Digital Era," McKinsey & Company, giugno 2020.
Disponibile su:https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20in%20a%20digital%20era/Cybersecurity%20in%20a%20Digital%20Era.pdf

[2] Gauran Banga, "How to Create a Dream Team for the New Age of Cybersecurity." Dark Reading, febbraio 2020.
Disponibile su: https://www.darkreading.com/cloud/how-to-create-a-dream-team-for-the-new-age-of-cybersecurity/a/d-id/1333849

[3] Cybersecurity Ventures Official Annual Cybercrime Report 2019.

[4] "Reinventing Cybersecurity with Artificial Intelligence," Capgemini Research Institute.
Disponibile su: https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

[5] Teju Shyamsundar, "AI Is Changing Security—Here's How," Okta Blog, gennaio 2020.
Disponibile: https://www.okta.com/blog/2020/01/ai-is-changing-security-heres-how/

[6] Zak Doffman, "Cyberattacks On IoT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims," Forbes, settembre 2019.
Disponibile su: https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#281bde785892

[7] Cisco Annual Internet Report (2018–2023) White Paper , marzo 2020
Disponibile su: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[8] "Cybersecurity CEO: The World Will Need to Cyber Protect 100X More Cloud Data by 2021," Cybersecurity CEO, Herjavec Group, ottobre 2018.
Disponibile su: https://www.robertherjavec.com/cybersecurity-ceo-cyber-protect-100x-cloud-data/

[9] Micheal Nadeau, "General Data Protection Regulation (GDPR): What you need to know to stay compliant," CSO, giugno 2020.
Disponibile: https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

[10] "Cyber-Risk Oversight Handbook For Corporate Boards," OAS.

[11] Chenxi Wang, "Corporate Boards Are Snatching Up Cybersecurity Talents," Forbes, agosto 2019.
Disponibile su: https://www.forbes.com/sites/chenxiwang/2019/08/30/corporate-boards-are-snatching-up-cybersecurity-talents/#615246a479f5

[12] https://www.venturescanner.com/2020/03/12/ai-2019-funding-achieved-banner-year/

[13] https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

Informazioni importanti:
** Non si intende raccomandare o sollecitare l'acquisto o la vendita di alcun titolo specifico. Un titolo menzionato in via esemplificativa potrebbe non essere più presente nel portafoglio del fondo alla data di pubblicazione del presente documento o ad una qualsiasi data successiva.*

L'investimento implica dei rischi. Il valore di un investimento e il reddito che ne deriva possono aumentare così come diminuire e, al momento del rimborso, l'investitore potrebbe non ricevere l'importo originariamente investito.