Otto elementi essenziali della sicurezza informatica

Pubblicato il 15 aprile 2024

Mobeen Tahir
Director, Research

Principali insegnamenti

- Con l'adozione di strumenti digitali da parte delle organizzazioni, i rischi legati alla sicurezza informatica sono in aumento.
- Dalla protezione dei dati ai dispositivi, fino alla formazione delle persone, questo è un campo dalle molteplici sfaccettature.
- Le aziende che si concentrano su più aree della sicurezza informatica hanno maggiori possibilità di resistere in un settore in rapida evoluzione.
- Prodotti correlati WisdomTree Cybersecurity UCITS ETF – USD Acc Scopri di più

Il 19 febbraio, il Financial Times ha riferito1 che alcuni criminali informatici nordcoreani avevano fatto ricorso all'intelligenza artificiale (IA) per rubare fondi e tecnologie all'avanguardia a vittime di tutto il mondo. Il report affermava che gli hacker avevano preso di mira aziende mondiali del settore della difesa, della sicurezza informatica e della crittografia, ingannando le persone su piattaforme popolari come LinkedIn. Inoltre, OpenAI, sviluppatore di ChatGPT, e Microsoft, suo investitore, hanno confermato che i malintenzionati stavano utilizzando i loro servizi di IA per attività informatiche dolose.

Gli strumenti di IA generativa hanno consentito alle persone di compiere operazioni più sofisticate dal punto di vista tecnico con competenze relativamente basilari. I modelli linguistici di grandi dimensioni permettono agli utenti di comunicare con il computer in una lingua come l'inglese, traducendo poi i loro comandi per scrivere programmi. Sfortunatamente, la tecnologia può anche consentire ai malintenzionati di compiere azioni illecite con maggiore facilità. Per questo motivo la sicurezza informatica deve diventare più intelligente e arginare tutte le potenziali vulnerabilità prima che i criminali le sfruttino.

WisdomTree ha collaborato con il venture group Team8 per identificare otto aree distinte della sicurezza informatica, essenziali in un mondo in cui i rischi sono in costante aumento.

Per essere esaustiva, la sicurezza informatica deve essere olistica

Fonte: WisdomTree, Team8, 2024.

Sicurezza dei dati

Si stima che il mondo produca 328 milioni di terabyte di dati ogni singolo giorno. Un terabyte corrisponde a 1000 gigabyte. In altre parole, il mondo sta producendo una mole di dati enorme. Inoltre, lo sta facendo più velocemente che mai. Si stima inoltre che il 90% dei dati mondiali sia stato generato solo negli ultimi due anni2.

IBM afferma che il costo medio di una violazione dei dati nel 2023 è stato di 4,45 milioni di dollari, con un aumento del 15% in tre anni3. Dato che il mondo produce più dati che mai, la loro protezione è fondamentale. L'obiettivo della sicurezza dei dati è proprio questo.

Sicurezza del cloud

Una produzione di dati tanto elevata comporta la necessità di aumentare lo spazio di archiviazione nel cloud. Secondo un report4, nello stesso viene archiviato circa il 60% di tutti i dati aziendali, rispetto ad appena il 30% del 2015. Inoltre, l'89% delle organizzazioni utilizza un approccio “multi-cloud”, un termine che si riferisce a un'azienda che si serve di almeno due applicazioni basate sul cloud.

E purtroppo i malintenzionati ne sono pienamente consapevoli. Nel 2023 i casi che sfruttano il cloud sono aumentati del 110%5. Questo significa che i criminali informatici provano sempre più spesso ad attaccare i loro bersagli attraverso applicazioni basate sullo stesso. Proteggerlo è quindi fondamentale per la sicurezza informatica.

Sicurezza anticipata

Non è possibile pensare di mettere in sicurezza il cloud o qualsiasi altra applicazione in un secondo momento. Per "sicurezza anticipata" si intende l'idea di integrare la sicurezza informatica nello sviluppo del software. Non farlo significherebbe applicarla in un secondo momento, affidandosi a soluzioni generiche di fornitori terzi.

La sicurezza anticipata consente agli sviluppatori di valutare in modo critico le vulnerabilità all'interno di un software per assicurarsi che al momento della sua creazione siano già presenti tutte le misure necessarie. In questo modo è possibile ridurre i costi e accelerare la fornitura, dato che, con tutta probabilità, il software che verrà presentato agli utenti porrà meno problemi.

Sicurezza più intelligente

L'IA generativa semplifica le operazioni dei malintenzionati. Creare codice doloso, come quello utilizzato in un attacco polimorfico, in grado di modificare il codice, il contenuto e la struttura per eludere i sistemi di sicurezza, è più facile che mai. Se viene bloccato da un'azienda, tale codice si ripresenta più forte.

Per affrontare queste minacce è necessario ricorrere all'automazione. Una sicurezza più intelligente prevede strumenti di automazione in grado di monitorare le reti alla ricerca di potenziali minacce. È qui che gli strumenti di intelligenza artificiale che imparano, si adattano e si evolvono giocano un ruolo cruciale nel garantire la sicurezza.

Sicurezza degli oggetti

L'Internet of Things (IoT) fa riferimento ai dispositivi connessi a internet. Computer portatili e telefoni cellulari sono esempi ovvi, sebbene ormai anche le automobili, gli orologi, gli assistenti digitali, le TV e le lavastoviglie, solo per citarne alcuni, facciano sempre più spesso parte dell'universo IoT. Si stima che, attualmente, al mondo ci siano 17 miliardi di dispositivi IoT e tale numero potrebbe raddoppiare entro il 20306.

Ovviamente, i nostri dispositivi devono essere protetti in quanto offrono ai malintenzionati punti di accesso alle nostre reti e ai nostri dati. La sicurezza degli oggetti, quindi, si basa sull'idea di proteggere tale numero crescente di dispositivi connessi da potenziali minacce.

Il mondo senza confini

La cosiddetta superficie di attacco è cresciuta dato che, dopo la pandemia di COVID-19, le organizzazioni hanno un numero maggiore di dipendenti che lavorano in remoto. Per superficie di attacco si intende l'insieme delle vulnerabilità che gli hacker possono sfruttare per accedere alla rete o ai dati sensibili di un'organizzazione. Rispetto al passato, in cui i lavoratori potevano essere circoscritti all'interno di un confine, oggi gli attaccanti hanno a disposizione un maggior numero di potenziali punti di accesso.

In un mondo senza confini, le organizzazioni hanno bisogno di strumenti più sofisticati per proteggersi. Tra questi, vi sono l'autenticazione a due fattori e i dati biometrici per gli utenti che accedono alla rete e alle applicazioni aziendali.

Resilienza e ripristino

A maggio 2017, l'attacco ransomware WannaCry è costato al Servizio sanitario nazionale del Regno Unito 92 milioni di sterline tra perdita di servizi e costi informatici. Ancor più significativo è il fatto che 19.000 appuntamenti siano stati cancellati a causa dell'interruzione dell'attività di oltre 80 ospedali e dell'8% degli studi medici di base7.

Secondo Team8, la sicurezza informatica non può limitarsi a "identificare, proteggere, rilevare e rispondere", ma deve anche prevedere la possibilità di eseguire un ripristino rapido nell'eventualità di degrado, interruzione o negazione dell'accesso alla rete o ai dati di un'organizzazione. In caso contrario, i costi possono essere catastrofici.

Un'organizzazione può disporre degli strumenti di sicurezza informatica più potenti per proteggersi. Ma se gli esseri umani non sono formati e dotati di mezzi per gestire i rischi, le relative misure possono sgretolarsi come un castello di sabbia. Il layer 8, quindi, è il fattore umano.

Secondo CrowdStrike, nel 2023 il 75% degli attacchi non conteneva malware, rispetto al 40% nel 2019. Questo significa che gli attaccanti si affidano meno agli attacchi malware trasmessi tramite e-mail di phishing e utilizzano metodi più sofisticati come l'ingegneria sociale, che hanno lo scopo di ingannare gli esseri umani. Pertanto, mettere le persone in condizione di gestire meglio i rischi della sicurezza informatica può essere alla base di tutte le altre misure.

Conclusione

La sicurezza informatica non è facoltativa. La sua importanza diventa fin troppo evidente nel momento in cui si verifica un attacco andato a segno. Ma a quel punto potrebbe essere troppo tardi per prevenire danni significativi. Un quadro di riferimento per la sicurezza informatica che adotti un approccio olistico a questi otto elementi essenziali può dare alle organizzazioni maggiori possibilità di evitare esiti indesiderati.

1 https://www.ft.com/content/728611e8-dce2-449d-bb65-cff11ac2a5bb
2 Preso da explodingtopics.com a dicembre 2023, che cita Statista come fonte delle informazioni. Explodingtopics.com/blog/data-generated-per-day
3 Report “Cost of a Data Breach 2023”, IBM.
4 Preso da explodingtopics.com a novembre 2023, che cita il Thales Group come fonte delle informazioni. Explodingtopics.com/blog/corporate-cloud-data
5 “2024 Global Threat Report”, CrowdStrike.
6 Explodingtopics.com a febbraio 2024, che cita Transforma Insights come fonte di informazioni. Explodingtopics.com/blog/number-of-iot-devices
7 National Health Executive, ottobre 2018.

Important Risks Related to this Article

INFORMAZIONI IMPORTANTI

Comunicazioni di marketing emesse all¼interno dello Spazio economico europeo ("SEE")¦ Il presente documento è stato emesso e approvato da WisdomTree Ireland Limited, società autorizzata e regolamentata dalla Central Bank of Ireland.

Comunicazioni di marketing emesse in giurisdizioni non appartenenti al SEE: Il presente documento è stato emesso e approvato da WisdomTree UK Limited, società autorizzata e regolamentata dalla Financial Conduct Authority del Regno Unito.

Per fare riferimento a WisdomTree Ireland Limited e a WisdomTree UK Limited si utilizza per entrambe la denominazione "WisdomTree" (come applicabile). La nostra politica sui conflitti d¼interesse e il nostro inventario sono disponibili su richiesta.

Solo per clienti professionali. I rendimenti ottenuti nel passato non sono un¼indicazione aidabile dei rendimenti futuri. I rendimenti storici ricompresi nel presente documento potrebbero essere basati sul back test, ossia la procedura di valutazione di una strategia d¼investimento, che viene applicata ai dati storici per simulare quali sarebbero stati i rendimenti di tale strategia. I rendimenti basati su back test sono puramente ipotetici e vengono forniti nel presente documento a soli fini informativi. I dati basati sul back test non rappresentano rendimenti eettivi e non devono intendersi come un¼indicazione di rendimenti eettivi o futuri. Il valore di un investimento potrebbe essere oggetto di oscillazioni dei tassi di cambio. Qualsiasi decisione d¼investimento deve essere basata sulle informazioni contenute nel Prospetto informativo di riferimento e deve essere presa dopo aver richiesto il parere di un consulente d¼investimento, fiscale e legale indipendente. I suddetti prodotti potrebbero non essere disponibili nel Suo mercato o adatti alle Sue esigenze. Il contenuto del presente documento non costituisce una consulenza in materia di investimenti, né un¼oerta di vendita o una sollecitazione di un¼oerta di acquisto di un prodotto o di sottoscrizione di un investimento.

Un investimento in exchange-traded product ("ETP") dipende dalla performance dell¼indice sottostante, sottratti i costi, ma diicilmente replicherà la performance dell¼indice con assoluta precisione. I prodotti ETP comportano numerosi rischi inclusi, tra gli altri, rischi generali di mercato correlati all¼indice sottostante di riferimento, rischi di credito riferiti al provider degli swap sull¼indice utilizzati nell¼ETP, rischi di cambio, rischi da tasso d¼interesse, rischi d¼inflazione, rischi di liquidità, rischi legali e normativi.

Le informazioni contenute nel presente documento non sono, e in nessun caso devono essere interpretate come, un annuncio pubblicitario o un altro strumento di promozione di un¼oerta pubblica di azioni negli Stati Uniti o in qualsiasi provincia o territorio degli stessi, laddove nessuno degli emittenti o dei relativi prodotti sia autorizzato o registrato per la distribuzione e laddove nessun prospetto di uno qualsiasi degli emittenti sia stato depositato presso una commissione di vigilanza o autorità di regolamentazione. Nessun documento, o informazione contenuta nel presente documento, deve essere estrapolato, trasmesso o distribuito (direttamente o indirettamente) negli Stati Uniti. Nessuno degli Emittenti né alcun titolo da essi

emesso sono stati o saranno registrati ai sensi dello United States Securities Act del 1933 o dell¼Investment Company Act del 1940 o qualificati ai sensi di qualsiasi legge statale sui titoli applicabile.

Il presente documento può contenere commenti indipendenti sul mercato redatti da WisdomTree sulla base delle informazioni disponibili al pubblico. Benché WisdomTree si adoperi per garantire l¼esattezza del contenuto del presente documento, WisdomTree non garantisce né assicura la sua esattezza o correttezza. Qualsiasi terzo fornitore di dati di cui ci si avvalga per reperire le

informazioni contenute nel presente documento non rilascia alcuna garanzia o dichiarazione di sorta in relazione ai suddetti dati. Laddove WisdomTree abbia espresso dei pareri relativamente al prodotto o all¼attività di mercato, si ricorda che tali pareri possono cambiare. Né WisdomTree, né alcuna consociata, né alcuno dei rispettivi funzionari, amministratori, partner o dipendenti, accetta alcuna responsabilità per qualsiasi perdita, diretta o indiretta, derivante dall¼utilizzo del presente documento o del suo contenuto.

Il presente documento può contenere dichiarazioni previsionali, comprese dichiarazioni riguardanti le nostre convinzioni o le nostre attuali aspettative in relazione alla performance di determinate classi di attività e/o settori. Le dichiarazioni previsionali sono soggette a determinati rischi, incertezze e ipotesi. Non vi è alcuna garanzia che tali dichiarazioni siano esatte, e i risultati eettivi possano discostarsi significativamente da quelli previsti in dette dichiarazioni. WisdomTree raccomanda vivamente di

non fare indebito aidamento sulle summenzionate dichiarazioni previsionali.

WisdomTree Issuer ICAV

I prodotti illustrati nel presente documento sono emessi da WisdomTree Issuer ICAV (l'"Emittente WT"). L¼Emittente WT è una società d¼investimento multicomparto a capitale variabile e con separazione delle passività tra comparti, costituita ai sensi del diritto irlandese come un veicolo di gestione patrimoniale collettiva irlandese e autorizzata dalla Central Bank of Ireland ("CBI"). L¼Emittente WT è costituito come Organismo d¼Investimento Collettivo in Valori Mobiliari ("OICVM") ai sensi del diritto irlandese ed emetterà una classe distinta di azioni (le "Azioni") per ciascun comparto. Si consiglia ai potenziali investitori di leggere il prospetto informativo dell'Emittente WT (il "Prospetto WT") prima di eettuare qualsiasi investimento e di riferirsi al capitolo intitolato "Fattori di rischio", per avere ulteriori informazioni in merito ai rischi associati all¼investimento nelle Azioni.

Per gli Investitori in Svizzera – Invesitori Qualificati

Questo documento costituisce una pubblicità dei prodotti finanziari qui menzionati.

Il prospetto e i documenti di informazioni chiave per gli investitori (KIID) sono disponibili sul sito Web di WisdomTree: **https:** //www.wisdomtree.eu/it-ch/resource-library/prospectus-and-regulatory-reports

Alcuni comparti di cui al presente documento potrebbero non essere stati registrati presso l¼Autorità federale di vigilanza sui mercati finanziari (“FINMA”). In Svizzera, i comparti che non sono stati registrati presso la FINMA saranno distribuiti esclusivamente a investitori qualificati, definiti nella legge svizzera sugli investimenti collettivi di capitale (LICo) ovvero nella sua ordinanza di attuazione (e singolarmente

modificate di volta in volta). Il rappresentante e agente per i pagamenti dei comparti in Svizzera è Société Générale Paris, Filiale di Zurigo, Talacker 50, PO Box 5070, 8021 Zurigo, Svizzera. Il prospetto, il documento contenente le informazioni chiave per gli investitori (KIID), lo statuto e le relazioni annuali e semestrali dei comparti sono disponibili gratuitamente presso il rappresentante e agente per i pagamenti svizzero. Con riferimento alla distribuzione in Svizzera, il luogo di giurisdizione e prestazione del servizio è la sede del rappresentante e agente per i pagamenti.

Per investitori francesi

Le informazioni riportate nel presente documento sono destinate esclusivamente agli investitori professionali (secondo quanto definito dalla MiFID) che investono per proprio conto e ne è vietata la distribuzione al pubblico. La distribuzione del Prospetto e l'oerta, la vendita e la consegna di Azioni

in altre giurisdizioni possono essere soggette a restrizioni di legge. L'Emittente è un OICVM di diritto irlandese, approvato dall¼Autorità di Vigilanza Finanziaria come OICVM conforme alle normative europee, sebbene potrebbe non essere tenuto ad adempiere alle stesse disposizioni vigenti per un prodotto simile approvato in Francia. Il Fondo è stato registrato per la commercializzazione in Francia dall¼Autorità dei Mercati Finanziari (Autorité des Marchés Financiers) e può essere distribuito agli investitori in Francia. Le copie di tutti i documenti (ovvero il Prospetto, il Documento contenente le informazioni chiave per gli investitori, eventuali supplementi o appendici, le ultime relazioni annuali, l'Atto costitutivo e lo Statuto) sono disponibili, gratuitamente, presso l'agente centralizzatore francese, Societe Generale con sede in 29, boulevard Haussmann – 75009 Parigi, Francia. La sottoscrizione delle Azioni del Fondo sarà eettuata conformemente alle condizioni indicate nel Prospetto e in eventuali integrazioni o appendici.

Per Investitori Maltese

Questo documento non costituisce o forma parte di qualsiasi oerta od invito alla pubblica sottoscrizione o acquisto di quote nel Fondo, non potrà essere interpretato come tale e nessuna persona al di fuori di quella al quale questo documento stato indirizzato od inviato sarà considerata come potenziale sottoscrittore di quote nel Fondo. Le quote del fondo non verranno commercializzate in alcun modo al pubblico a Malta senza la precedente autorizzazione dell¼Autorità Finanziaria Maltese.