

Mettere in sicurezza il mondo post-AI per i servizi finanziari con Zero Trust

Un approccio strategico alla sicurezza informatica nell'era dell'AI

PANORAMICA SULLA SOLUZIONE

© 2024 Zscaler, Inc. Tutti i diritti riservati.

Sintesi esecutiva: navigare nella foresta oscura

In un mondo post–AI, i servizi finanziari devono orientarsi in una "foresta oscura" di minacce nascoste e incertezze, dove ogni interazione può rappresentare un rischio. Così come si eserciterebbe la massima cautela in un ambiente pericoloso e imprevedibile, i servizi finanziari devono affrontare la sicurezza AI con vigilanza. Questo breve documento illustra i passi che le organizzazioni di servizi finanziari possono intraprendere per proteggersi mentre entrano in questo scenario guidato dall'AI.

Esploreremo come l'AI stia rimodellando il panorama delle minacce, introducendo nuove vulnerabilità come le frodi basate sull'AI e gli attacchi informatici automatizzati. Inoltre, evidenzieremo tendenze e previsioni chiave, aiutando le organizzazioni ad anticipare l'impatto dell'AI e a rispondere in modo strategico.

La migliore difesa in questo ambiente ad alto rischio, dove nessuna entità (sia interna che esterna all'organizzazione) può essere considerata affidabile, è il modello zero trust. Questo documento fornisce un percorso chiaro affinché le organizzazioni di servizi finanziari possano iniziare il loro percorso verso lo zero trust, offrendo passi concreti per garantire un futuro AI sicuro e resiliente.

L'AI e il panorama di minacce in continua evoluzione

L'AI sta trasformando rapidamente il panorama delle minacce, introducendo rischi complessi che mettono in discussione i modelli di sicurezza tradizionali. Gli attacchi si sono evoluti e sono diventati più efficaci su larga scala, consentendo alle vittime di continuare a operare mentre gli aggressori minacciano di esporre i loro dati. Sebbene esistano molte mega tendenze e previsioni legate all'AI, ci concentreremo su tre tendenze per il 2024–2025 che si sono evolute a un ritmo più rapido.

2024–2025 Tre tendenze da tenere d'occhio

Sviluppo dell'intelligenza artificiale della sequenza principale

I modelli linguistici di grandi dimensioni (LLM) hanno trasformato il modo in cui pensiamo alla generative AI, espandendo le sue capacità oltre output ristretti e specifici per attività verso soluzioni più dinamiche e consapevoli del contesto. Ma proprio come il mondo reale, tutto, compresa l'AI, continuerà a evolversi. Questi LLM ci hanno catturati una volta superata la "valle perturbante".

La "valle perturbante" si riferisce alla sensazione di disagio che le persone provano quando l'AI diventa quasi (ma non del tutto) indistinguibile dagli esseri umani, generando disagio a causa della sua imitazione quasi perfetta.

La GenAI, e in particolare ChatGPT, ha superato la valle perturbante quando ha raggiunto 100 milioni di utenti in due mesi, il che è straordinario. Ora che ha superato la valle perturbante, c'è altro in arrivo che potrebbe avere un impatto maggiore dal punto di vista neurologico e cognitivo rispetto alla sola GenAI.

Attacchi ransomware senza crittografia

In precedenza la crittografia veniva utilizzata per i ransomware: l'agenda principale era rubare i tuoi dati, tenere in ostaggio le tue operazioni e, se non pagavi, non potevi mandare avanti l'attività.

© 2024 Zscaler, Inc. Tutti i diritti riservati.

Tuttavia, col tempo, gli aggressori che sfruttano i ransomware si sono resi conto che, abbassando la cifra richiesta e non impedendo alla vittima di fare affari, avrebbero ottenuto un rendimento più alto. Ad esempio, se il riscatto scende da 10 milioni a 2 milioni e si passa da una probabilità del 5% di pagamento a una probabilità del 70–80%, diventa un modello di business ransomware "migliore" su larga scala. Questo è il ransomware senza crittografia.

Nel ransomware senza crittografia rubano i dati, ti minacciano e in molti casi ti permettono di continuare le operazioni perché non vogliono fermare la tua attività.

Non interrompendo il business, i danni reputazionali possono essere inferiori. Gli aggressori possono anche cercare di convincere la vittima a non denunciare il riscatto alla SEC/regolatore perché non è considerato sufficientemente rilevante.

Attacchi ransomware basati su AI

Gli attacchi ransomware basati su AI sono più efficaci nel migliorare il rendimento, la penetrazione e l'automazione degli attacchi. In questo caso, gli aggressori sfruttano l'AI per automatizzare e aumentare la sofisticazione degli attacchi informatici, rendendoli più rapidi, mirati e difficili da rilevare.

Quattro modi in cui i servizi finanziari possono navigare nello scenario AI in evoluzione

L'uso aziendale dell'AI è in forte crescita, insieme ai rischi. I quattro livelli di considerazione strategica aziendale possono guidare le organizzazioni di servizi finanziari nell'affrontare le complessità di un mondo post–AI in continua evoluzione.

Nel 2024, l'uso di strumenti AI/ML è cresciuto del 594% e l'uso di ChatGPT è salito al 634% (Report di Zscaler ThreatLabz del 2024 sulla sicurezza dell'AI).

Policy ed etica

I servizi finanziari devono sviluppare policy complete che regolino l'uso etico dell'AI, garantendo la conformità normativa e favorendo la fiducia dei clienti. Ciò implica la creazione di un quadro che affronti la privacy dei dati, la trasparenza algoritmica e la mitigazione dei bias, sottolineando pratiche di AI responsabile.

Core business

In che modo l'intelligenza artificiale impatta sul core business? L'Harvard Business Review ha condotto uno studio che ha mostrato una differenza statisticamente significativa nelle performance delle aziende che usano l'AI rispetto a quelle che non la usano nello stesso settore, e questo divario continua ad ampliarsi.

Quindi, come intendi introdurre l'AI nel business? Lo farai con un partner o in modo indipendente? Intendi possedere modelli tuoi? Intendi partecipare a modelli più grandi? E qual è il caso d'uso in questione?

Le organizzazioni dovrebbero valutare come l'AI può migliorare le operazioni principali, come il miglioramento dei servizi ai clienti, l'ottimizzazione dei processi e l'abilitazione di decisioni basate sui dati.

© 2024 Zscaler, Inc. Tutti i diritti riservati.

Le organizzazioni dovrebbero valutare come l'AI può migliorare le operazioni principali, come il miglioramento dei servizi ai clienti, l'ottimizzazione dei processi e l'abilitazione di decisioni basate sui dati. Identificando le aree chiave in cui l'AI può apportare valore, le organizzazioni di servizi finanziari possono creare vantaggi competitivi e stimolare l'innovazione in linea con gli obiettivi strategici.

R&S e infrastrutture

Man mano che gli strumenti AI entrano nel business, come gestirli? Investire in un'infrastruttura solida che supporti le capacità AI, come cloud computing, big data analytics e machine learning, consentirà alle organizzazioni di sfruttare le tecnologie emergenti e sviluppare nuove soluzioni per soddisfare le esigenze in evoluzione dei clienti.

Vantaggi della sicurezza informatica

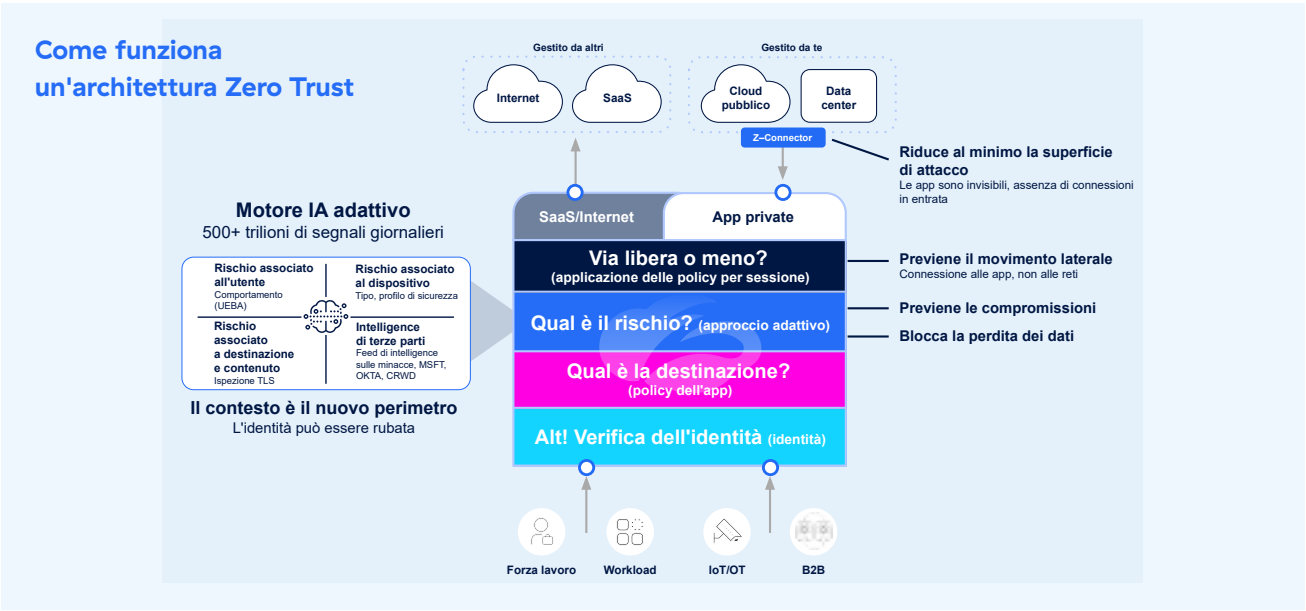
Le istituzioni finanziarie possono rafforzare il loro profilo di sicurezza informatica utilizzando soluzioni di sicurezza che sfruttano l'AI per identificare e rispondere alle minacce in tempo reale.

Ci sono alcune domande che dovresti porti: quali sono i vantaggi dell'AI per la sicurezza informatica o potenzialmente le minacce? Come verrà usata contro di te? Come puoi prepararti? Implementando misure di sicurezza basate su AI, le organizzazioni possono proteggere meglio dati e asset sensibili e garantire resilienza contro minacce sofisticate.

Il ruolo dello zero trust nella riduzione del rischio informatico

Anche se l'uso aziendale dell'AI accelera, le imprese bloccano il **18,5%**di tutte le transazioni AI, un aumento del **577%** che segnala crescenti preoccupazioni per la sicurezza (Report di Zscaler ThreatLabz del 2024 sulla sicurezza dell'AI). La migliore difesa in questo ambiente ad alto rischio, dove nessuna entità (sia interna che esterna all'organizzazione) può essere considerata affidabile, è lo zero trust.

Lo zero trust è la strategia che ci aiuta a navigare nella foresta oscura consentendo solo ciò che il business richiede quando lo richiede. Implementare un approccio zero trust garantisce che, indipendentemente da utente, workload, dispositivo o altra azienda, tu possa ridurre significativamente il rischio informatico:



© 2024 Zscaler, Inc. Tutti i diritti riservati.

1. Autenticare l'identità: stop! Chi sei?

a. Chi si sta connettendo?

b. Quali sono gli attributi?

c. Qual è la destinazione della connessione?

2. Controllare le policy delle app: dove stai cercando di andare?

a. Dove stai cercando di andare? In questo passaggio, lo zero trust valuta il rischio utilizzando il contesto, prevenendo compromissioni e perdita di dati.

3. Rischio contestuale adattivo: qual è il rischio?

a. Qual è il rischio? Previeni compromissioni e ferma la perdita di dati valutando il rischio utente, il rischio del dispositivo, la destinazione, il rischio del contenuto e le informazioni da terze parti (Okta, CrowdStrike, ecc.).

4. Applica le policy

a. Previeni i movimenti laterali in modo da connetterti alle app, non alle reti

b. Applica policy sia per connessioni SaaS/internet basate su sessione e utente

c. Applicazioni private: minimizza la superficie d'attacco affinché le app siano invisibili e non possano avvenire connessioni in entrata.

Un percorso verso lo zero trust

Per proteggere la tua azienda dal crescente numero di minacce informatiche alimentate dall'AI, intraprendere un percorso zero trust è essenziale. Implementare un percorso zero trust deve essere visto come un processo graduale, suddiviso in passaggi gestibili che si allineano alle priorità aziendali e agli obiettivi di sicurezza, garantendo che la tua sicurezza evolva in modo scalabile e resiliente.

1. Proteggi la forza lavoro

a. Fase 1A—nessun cambiamento di rete

i. Protezione informatica e dei dati, esperienza digitale e quantificazione del rischio

b. Fase 1B—semplificazione della rete

i. Ufficio filiale zero trust/internet café, strategia avanzata di protezione informatica e dei dati, e ottenere informazioni aziendali

2. Carichi di lavoro sicuri

a. Protezione informatica e dei dati per i workload

b. Rete e segmentazione dei workload zero trust

3. Accesso di terze parti

a. Accesso alle app di terze parti con zero trust

b. Connettività ai siti di terze parti con zero trust

4. Mettere in sicurezza i dispositivi (IoT/OT)

a. Protezione informatica e dei dati per IoT/OT

b. Connettività IoT/OT con zero trust

© 2024 Zscaler, Inc. Tutti i diritti riservati.

Conclusione

Lo zero trust offre la migliore difesa in questo scenario in rapida evoluzione, dove nessuna entità (sia interna che esterna all'organizzazion) può essere intrinsecamente affidabile. Con la tecnologia e l'AI che continuano a evolversi e infine a convergere, adottare una strategia zero trust assicura che solo gli utenti e i processi corretti accedano a ciò che serve e quando serve, garantendo resilienza e preparando la tua organizzazione al futuro.

Riduci il tuo rischio informatico, inizia il tuo percorso zero trust imparando di più su zscaler.com/it

Conosci l'autore



Con oltre 3 decenni come imprenditore, esperto di sicurezza informatica ed executive in aziende come RSA, Arbor Networks, CA, McAfee, Cybereason e altre, Sam è dedicato a rafforzare i difensori nei conflitti informatici e a realizzare la promessa della sicurezza, rendendo possibile un mondo sicuro, affidabile e connesso. Attualmente, Sam Curry è Global VP, CISO presso Zscaler e nel tempo libero è relatore pubblico, conduce un podcast (On the Hook), siede in vari board e pubblicazioni, ed è un mentore InfoSec. Connettiti con me su LinkedIn.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.com/it** o seguici su X (precedentemente Twitter) **sull'account @zscaler**.

©2024 Zscaler, Inc. Tutti i diritti riservati. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ e ZPA™ e gli altri marchi commerciali indicati su **zscaler.com/it/legal/trademarks** sono (I) marchi commerciali o marchi di servizio registrati o (II) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi commerciali sono di proprietà dei rispettivi titolari.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/it