Published on Camera di Commercio di Messina (https://me.camcom.it)



Lunedì 6 Ottobre 2025 Notizie [1]

Dizionario di Cybersecurity

Conosci l'Input Perturbation Attack?

Nel mondo della cyber security aziendale, le minacce evolvono costantemente. Uno degli attacchi più subdoli e tecnicamente sofisticati degli ultimi anni è l'**Input Perturbation Attack**.

Questo tipo di attacco prende di mira i sistemi di intelligenza artificiale e machine learning (Al/ML), sempre più utilizzati dalle imprese per automatizzare processi, analizzare dati e prendere decisioni.

In questo articolo esploreremo cos'è un Input Perturbation Attack, come può colpire le aziende e come difendersi.

Cos'è un Input Perturbation Attack

Un **Input Perturbation Attack**, noto anche come **attacco avversarial**, è una tecnica attraverso cui un attaccante modifica impercettibilmente i dati in input a un sistema di intelligenza artificiale per ottenere un risultato errato o manipolato.

Queste perturbazioni sono **quasi invisibili a occhio nudo**, ma sufficienti a confondere modelli Al anche molto avanzati. Un classico esempio: un'immagine di un semaforo leggermente alterata che viene classificata erroneamente da un sistema di guida autonoma come un cartello stradale.

Perturbation Attack: come avvengono gli attacchi alle imprese

Published on Camera di Commercio di Messina (https://me.camcom.it)

Le imprese sono sempre più dipendenti da sistemi basati su Intelligenza Artificiale e Machine Learning per attività come:

- Riconoscimento facciale nei sistemi di sicurezza;
- Analisi dei dati finanziari;
- Rilevamento delle frodi;
- · Diagnosi medica automatizzata;
- Controllo qualità automatizzato in ambito industriale.

Dunque, in un contesto aziendale, un attacco tramite Input Perturbation può portare a conseguenze gravi quali:

• Manipolazione dei risultati

un attacco al sistema antifrode di una banca può permettere il passaggio di transazioni fraudolente;

• Compromissione della sicurezza

nei sistemi biometrici, un volto contraffatto può superare i controlli d'accesso;

• Sabotaggio industriale

piccoli cambiamenti nelle immagini dei prodotti possono ingannare sistemi di controllo qualità, permettendo l'uscita di merce difettosa;

• Danni reputazionali

errori derivanti da modelli compromessi possono compromettere la fiducia di clienti e partner.

Chi sono gli autori di questi attacchi? Gli hacker possono essere sia esterni che insider, con accesso ai dati o al modello di Al da parte di chi è già dentro l'impresa.



Dizionario di Cybersecurity CAMERA DI COMMERCIO



Published on Camera di Commercio di Messina (https://me.camcom.it)

Come proteggere la tua impresa dagli Input Perturbation Attack

In un'epoca in cui l'intelligenza artificiale e i sistemi automatizzati stanno rivoluzionando il mondo del business, gli input perturbation attacks rappresentano una minaccia concreta e sofisticata che gli imprenditori non possono più ignorare.

Proteggersi da questi attacchi richiede un approccio proattivo e multilivello. Ecco alcune strategie chiave:

Difese adversarial-aware nei modelli Al

Integrare tecniche di Adversarial Training, che addestrano il modello a riconoscere e gestire input manipolati. È simile a un vaccino: si "espone" il modello a perturbazioni durante l'addestramento.

• Monitoraggio continuo degli input

Implementare sistemi che analizzano gli input in tempo reale alla ricerca di anomalie o segnali sospetti, ad esempio attraverso tecniche di anomaly detection.

· Difese a livello di sistema

Non affidarsi unicamente ai modelli Al. Integrazione di controlli ridondanti (es. verifica umana, logica aggiuntiva, controlli basati su regole) può prevenire decisioni errate.

• Blind test e audit periodici

Effettuare audit regolari sui modelli Al per testarne la robustezza contro attacchi adversariali. Utilizzare team red-team/blue-team per simulare attacchi reali.

• Data governance e sicurezza dei dati

Proteggere i dati di addestramento: se un attaccante riesce a compromettere questi dati, può influenzare il comportamento del modello. È essenziale implementare rigorose policy di data security.

Concludendo, possiamo dire che per proteggere la tua azienda dagli input perturbation attacks, è importante considerare la sicurezza come parte integrante delle tue strategie digitali. Coinvolgere esperti e aggiornarsi costantemente può fare la differenza nel preservare l'affidabilità dei sistemi basati su intelligenza artificiale. Ultima modifica: Lunedì 6 Ottobre 2025

Condividi Reti Sociali	
Gradimento	Nessun voto
Rate	

ARGOMENTI



Dizionario di Cybersecurity

Published on Camera di Commercio di Messina (https://me.camcom.it)

Source URL: https://me.camcom.it/notizie/dizionario-cybersecurity

Collegamenti

[1] https://me.camcom.it/notizie/%3Ffield_notizia_categoria_tid%3D385