DELL Technologies

5 Consigli per massimizzare in modo sicuro la GenAI

1	2	3	4	5
Proteggi i livelli di un sistema GenAI	**Usa i principi Zero Trust**	**Mantieni la governance e la supervisione umana**	**Sfrutta gli strumenti di sicurezza GenAI non appena saranno disponibili**	**Innova in tutta sicurezza**
Infrastruttura	Mai fidarsi, verificare sempre	Coinvolgi le entità interessate principali	Contenuti	Punta sulla sicurezza informatica per agevolare la missione, non per ostacolarla
Sistemi operativi e Kubernetes	Accesso con privilegi minimi	Definisci policy per la conformità etica e normativa e la gestione dei dati	Previsione del rischio	Lascia che la maturità della sicurezza informatica crei fiducia nell'organizzazione in materia di innovazione
Applicazioni GenAI	Consolidamento del sistema	Monitora e applica responsabilità	Conoscenza e automazione	
Dati	Gestione delle identità	Addestramento e formazione		
	Segmentazione			
	Registrazione, monitoraggio e verifica			

la tecnologia dell'intelligenza artificiale generativa promette capacità trasformative ma presenta delle proprie sfide di sicurezza.

l'intelligenza artificiale generativa sta rivoluzionando il business come mai prima d'ora, promuovendo l'innovazione e offrendo vantaggi senza precedenti che offrono un vantaggio competitivo. Sebbene questa tecnologia abbia un enorme potenziale di trasformazione, non è priva di sfide in termini di sicurezza.

Gli esperti in materia di Dell Steve Brodson, Services Product Manager ed Eitan Lederman, CyberSecurity Consultant, si sono uniti a Chris Cicotte dal team di marketing APEX e AI per rispondere a tali problemi e discutere dei modi per massimizzare in modo sicuro la GenAI. Continua a leggere per un riepilogo della conversazione e ulteriori approfondimenti sull'argomento e guarda la discussione completa all'indirizzo dell.com/cybersecuritymonth.

> Tutto sta nel formare le persone. Le persone devono sapere come utilizzare il sistema GenAI. Cosa fare, ma anche cosa non fare".
>
> ***Eitan Lederman***
> *Consulente per la sicurezza informatica Dell*

Proteggi i livelli di un sistema GenAI

Sebbene la GenAI sia una tecnologia relativamente nuova, la maggior parte dei protocolli di sicurezza sono le stesse tecniche di cybersicurezza consolidate utilizzate per proteggere altri carichi di lavoro.

Infrastruttura: focalizzazione sulla riduzione al minimo della superficie di attacco:

- Vulnerabilità e test di penetrazione
- Applicazione delle patch
- Rafforzamento
- Gestione delle identità, incluse password complesse, autenticazione a più fattori (MFA)
- Monitoraggio e verifica
- Garantire che la supply chain di terze parti sia sicura

OS e Kubernetes: attenzione particolare alla riduzione della superficie degli attacchi, tra cui:

- Analisi delle vulnerabilità
- Applicazione regolare di patch
- Aggiornamento dei componenti Kubernetes
- Limitazione del controllo degli accessi in base alla gestione delle identità, all'accesso basato sui ruoli (RBAC) e all'accesso con privilegi minimi
- Protezione del piano di gestione, inclusi il server API, i segreti, il kubelet e altri componenti
- Utilizzo di namespace

Applicazioni GenAI: implementa azioni di sicurezza mirate alle nuove superfici di attacco create dalla GenAI:

- Gestione delle identità per affrontare la prompt injection, la divulgazione di informazioni sensibili, il furto di modelli, l'inquinamento dei dati di formazione
- Convalida delle origini dati per la protezione da inquinamento dei dati di formazione, pregiudizi del modello
- Monitoraggio e verifica per identificare e prevenire DoS del modello, furto di modelli, divulgazione di informazioni sensibili, rilevamento di anomalie, analisi forensi

Dati: integra misure di protezione dei dati solide per proteggere i dati nel modello linguistico e nell'applicazione:

- Cyber Vault autosufficiente
- Crittografia
- Piano di risposta agli incidenti
- Monitoraggio e verifica dei dati di formazione e dei risultati

Assicurati che i principi di protezione dei dati siano applicati a tutti i dati, compresi gli input di formazione, gli output dei modelli e tutti i dati coinvolti nella Retrieval Augmented Generation (RAG), se applicabile. Inoltre, garantisci la conformità costante con tutte le normative sulla protezione dei dati applicabili.

Usa i principi Zero Trust

Il ruolo di diversi principi Zero Trust come la gestione delle identità, l'accesso con privilegi minimi, il consolidamento del sistema e l'applicazione di patch è già stato menzionato, a indicare il valore dei principi Zero Trust nella protezione di un carico di lavoro GenAI. Le architetture Zero Trust richiedono inoltre la registrazione, il monitoraggio e il controllo continui delle attività di rete, che possono prevenire rischi specifici della GenAI come la manipolazione dei risultati e l'inquinamento dei dati.

DELL Technologies

Inoltre, Zero Trust incoraggia anche la micro-segmentazione, ricend l'impatto di una violazione. Inoltre, richiede la crittografia dei dati, sia in transito sia a riposo, che rappresenta una parte importante della strategia globale di protezione dei dati.

Sebbene questi siano solo alcuni dei modi in cui Zero Trust può proteggere un carico di lavoro GenAI, l'adozione dei principi Zero Trust deve essere considerata una best practice.

Mantieni la governance e la supervisione umana

Gran parte del valore della GenAI risiede nell'automazione delle attività normalmente eseguite dagli esseri umani, ma la governance umana è fondamentale per garantire la sicurezza e il corretto funzionamento delle applicazioni. Un modello di governance normalmente coinvolge le principali entità interessate in tutta l'organizzazione, che stabiliscono linee guida e requisiti per la conformità etica e normativa, le policy e le procedure di gestione dei dati e, in ultima analisi, attribuiscono responsabilità.

Una governance e una supervisione appropriate possono favorire la risoluzione di problemi quali l'eccessiva dipendenza dal modello, i pregiudizi, la manipolazione dei risultati, la divulgazione di informazioni sensibili e l'inquinamento dei dati.

Lederman ha sottolineato anche l'importanza della formazione: "Tutto sta nel formare le persone. Le persone devono sapere come utilizzare il sistema GenAI. Cosa fare, ma anche cosa non fare".

Oltre al rischio rappresentato dalle applicazioni GenAI di un'organizzazione, è presente anche la proliferazione degli attacchi informatici basati sulla GenAI che spesso richiedono un intervento umano. Per esempio, gli autori di attacchi malevoli che utilizzano sistemi di deepfake per guidare il comportamento umano e gli attacchi di phishing, che sono più efficaci poiché simulano in modo più accurato lo stile di scrittura o di conversazione di un essere umano. Una formazione e un'istruzione continue rappresentano alcuni dei metodi più efficaci per affrontare i rischi correlati a questo problema, rafforzando ancora una volta il ruolo fondamentale dell'essere umano.

Sfrutta la GenAI negli strumenti di sicurezza non appena saranno disponibili

Sebbene la maggior parte dell'attenzione sia rivolta al rischio, la GenAI ha anche il potenziale per rafforzare gli sforzi di sicurezza. Sebbene queste funzionalità siano in stato embrionale, in futuro offriranno vantaggi in tre aree chiave:

- **Contenuto:** generazione di policy di sicurezza, formazione personalizzata, classificazione dei dati e reporting
- **Previsione:** del rischio e dell'attività di attacco, suggerimento di azioni correttive
- **Conoscenza:** interrogare l'ambiente (interagire con il sistema), analisi forense, automazione

Il contributo della GenAI agli strumenti di sicurezza potrebbe essere utile a massimizzare le capacità dei team di sicurezza, ridurre i costi e migliorare le difese. Sfrutta queste soluzioni man mano che crescono e maturano.

Innova in tutta sicurezza

Soprattutto, non lasciare mai che i rischi per la sicurezza ti impediscano di sfruttare tecnologie potenzialmente rivoluzionarie. Efficienza, automazione, riduzione dei costi, risoluzione dei problemi e promozione della creatività sono solo alcuni dei modi in cui la GenAI può trasformare il business.

sebbene la GenAI richieda misure di sicurezza informatica solide e talvolta nuove, l'obiettivo deve essere quello di facilitare la missione dell'organizzazione, non di ostacolarla. Lo sviluppo della giusta strategia di sicurezza informatica dovrebbe offrire alle organizzazioni la sicurezza necessaria per crescere e innovare.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi su **dell.com/cybersecuritymonth**

DELL Technologies