DELL Technologies

5 Empfehlungen für eine sichere Maximierung der GenAI-Nutzung

1	2	3	4	5
Sichern Sie die Schichten eines GenAI-Systems	**Nutzen Sie Zero-Trust-Prinzipien**	**Halten Sie die Governance und menschliche Aufsicht aufrecht**	**Nutzen Sie die Vorteile der GenAI-Sicherheits tools, sobald sie verfügbar sind**	**Treiben Sie Innovationen souverän voran**
Infrastruktur	Niemals vertrauen, immer verifizieren	Wichtige StakeholderInnen einbeziehen	Inhalt	Cybersicherheit soll die Mission erleichtern und nicht behindern
BS und Kubernetes	Zugriff nach dem Least-Privilege-Prinzip	Policies für die Einhaltung ethischer Vorgaben und behördlicher Auflagen sowie für das Datenmanagement festlegen	Risikoprognose	Cybersicherheit-sreifegrad zur Verstärkung des Vertrauens des Unternehmens in Innovationen
GenAI-Anwendungen	Härten des Systems	Verantwortlichkeit überwachen und durchsetzen	Wissen und Automatisierung	
Daten	Identitätsmanagement	Schulung und Weiterbildung		
	Segmentierung			
	Protokollierung, Monitoring und Auditing			

Die GenAI-Technologie verspricht transformative Fähigkeiten, bringt jedoch einzigartige Sicherheitsherausforderungen mit sich.

Generative KI (GenAI) revolutioniert Unternehmen wie nie zuvor. Sie fördert Innovationen und bietet beispiellose Vorteile, die für einen Wettbewerbsvorteil sorgen. Diese Technologie hat zwar transformatives Potenzial, bringt aber auch eine Reihe von Sicherheitsherausforderungen mit sich.

Die Dell Subject Matter Experts Steve Brodson, Services Product Manager, und Eitan Lederman, Cybersecurity Consultant, haben diese Bedenken gemeinsam mit Chris Cicotte vom APEX- und KI-Marketingteam diskutiert und Möglichkeiten zur sicheren Maximierung von GenAI erörtert. Lesen Sie weiter, um eine Zusammenfassung des Gesprächs und zusätzliche Einblicke in das Thema zu erhalten. Das vollständige Gespräch finden Sie unter dell.com/cybersecuritymonth.

> Es geht darum, MitarbeiterInnen zu schulen. Die MitarbeiterInnen müssen wissen, wie sie das GenAI-System nutzen – was zu tun ist, aber auch, was nicht getan werden sollte.“
>
> ***Eitan Lederman***
> *Dell Cybersecurity Consultant*

Sichern Sie die Schichten eines GenAI-Systems

Auch wenn GenAI eine relativ neue Technologie ist, handelt es sich bei den meisten Sicherheitsprotokollen um dieselben etablierten Cybersicherheitstechniken, die zur Sicherung anderer Workloads verwendet werden.

Infrastruktur – Fokussierung auf die Minimierung der Angriffsfläche:

- Sicherheitslückenbewertungen und Penetrationstests
- Patching
- Hardening
- Identitätsmanagement, einschließlich sicherer Kennwörter, Multi-Faktor-Authentifizierung (MFA)
- Monitoring und Überprüfung
- Sicherstellen einer sicheren Lieferkette von Drittanbietern

BS und Kubernetes – weitere Fokussierung auf die Reduzierung der Angriffsfläche, einschließlich:

- Schwachstellenscans
- Regelmäßiges Patchen
- Aktualisieren von Kubernetes-Komponenten
- Beschränkende Zugriffskontrolle basierend auf Identitätsmanagement, rollenbasiertem Zugriff (RBAC) und Zugriff mit der geringsten Berechtigung
- Sicheren der Steuerungsebene, einschließlich des API-Servers, der geheimen Schlüssel, des Kubelet und anderer Komponenten
- Verwenden von Namespaces

GenAI-Anwendungen – Implementierung von Sicherheitsmaßnahmen, die auf die von GenAI geschaffenen neuen Angriffsflächen ausgerichtet sind:

- Identitätsmanagement zur Vermeidung der Einschleusung von Prompts, Offenlegung vertraulicher Informationen, Modelldiebstahl und der Vergiftung von Trainingsdaten
- Datenquellenvalidierung zum Schutz vor Vergiftung von
- Trainingsdaten und Modellvoreingenommenheit

  Monitoring und Überprüfung zur Identifizierung und Verhinderung von

  Modell-DOS, Modelldiebstahl, Offenlegung vertraulicher Informationen, Anomalieerkennung, Forensik

Daten – Integration solider Data-Protection-Maßnahmen für den Schutz der Daten im Sprachmodell und in der Anwendung:

- Cyber-Vault mit Air Gap
- Verschlüsselung
- Incident-Reaktionsplan
- Monitoring und Überprüfung von Trainingsdaten und Ausgaben

Stellen Sie sicher, dass die Data-Protection-Prinzipien auf alle Daten angewendet werden, einschließlich Trainingseingaben, Modellausgaben und alle Daten, die an Retrieval Augmented Generation (RAG) beteiligt sind, falls diese Technologie verwendet wird. Sorgen Sie außerdem dafür, dass fortlaufend alle geltenden Datenschutzbestimmungen eingehalten werden.

Nutzen Sie Zero-Trust-Prinzipien

Die Rolle verschiedener Zero-Trust-Prinzipien wie Identitätsmanagement, Zugriff mit der geringsten Berechtigung, Härten des Systems und Patchen wurde bereits erwähnt und verdeutlicht den Wert von Zero-Trust-Prinzipien bei der Sicherung einer GenAI-Workload. Zero-Trust-Architekturen erfordern außerdem kontinuierliches Protokollieren, Monitoring und Überprüfen von Netzwerkaktivitäten, wodurch GenAI-spezifische Risiken wie Ergebnismanipulation und Datenvergiftung vermieden werden können.

DELL Technologies

Darüber hinaus fördert Zero Trust auch die Mikrosegmentierung, wodurch die Auswirkungen einer Sicherheitsverletzung reduziert werden. Außerdem ist eine Datenverschlüsselung sowohl während der Übertragung als auch im Ruhezustand erforderlich, die ein wichtiger Bestandteil der allgemeinen Data-Protection-Strategie ist.

Dies sind zwar nur einige der Möglichkeiten, wie Zero Trust eine GenAI-Workload schützen kann, aber die Einführung von Zero-Trust-Prinzipien sollte als Best Practice betrachtet werden.

Halten Sie die Governance und menschliche Aufsicht aufrecht

Ein Großteil des Mehrwerts von GenAI liegt in der Automatisierung von Aufgaben, die normalerweise von Menschen ausgeführt werden. Menschliche Governance ist jedoch kritisch, um für Sicherheit und eine ordnungsgemäße Funktionsweise der Anwendungen zu sorgen. An einem Governance-Modell sind in der Regel wichtige StakeholderInnen im gesamten Unternehmen beteiligt, die Richtlinien und Anforderungen für die ethische und behördliche Compliance sowie Datenmanagement-Policies und -verfahren festlegen und letztendlich die Verantwortlichkeit durchsetzen.

Eine angemessene Governance und Aufsicht können dazu beitragen, Probleme wie blindes Vertrauen auf das Modell, Voreingenommenheit, Ergebnismanipulation, Offenlegung vertraulicher Informationen und Datenvergiftung anzugehen.

Lederman weist auch auf die Bedeutung von Schulungen hin: „Es geht darum, MitarbeiterInnen zu schulen. Die MitarbeiterInnen müssen wissen, wie sie das GenAI-System nutzen – was zu tun ist, aber auch, was nicht getan werden sollte."

Zusätzlich zu den Risiken, die von den GenAI-Anwendungen eines Unternehmens ausgehen, gibt es auch die starke Zunahme von GenAI-fähigen Cyberangriffen, die oft menschliches Eingreifen erfordern. Beispiele hierfür sind böswillige AkteurInnen, die Deepfakes verwenden, um menschliches Verhalten zu steuern, und Phishingangriffe, die durch eine genauere Nachahmung des Schreib- oder Sprechstils eines Menschen viel effektiver werden. Kontinuierliche Schulung und Weiterbildung gehören zu den effektivsten Möglichkeiten, diesen Risiken zu begegnen und auch hier die menschliche Komponente zu stärken.

Nutzen Sie GenAI in Sicherheitstools, sobald sie verfügbar werden

Zwar liegt der Fokus vor allem auf Risiken, aber GenAI hat auch das Potenzial, Sicherheitsinitiativen zu verstärken. Die Funktionen stecken zwar noch in den Kinderschuhen, bieten aber Vorteile in drei wichtigen Bereichen:

- **Inhalt:** Erstellung von Sicherheits-Policies, personalisierte Schulungen, Datenklassifizierung und Reporting
- **Prognose:** Risiko- und Angriffsaktivitäten, Vorschläge für Korrekturmaßnahmen
- **Wissen:** Abfrage der Umgebung (Kommunikation mit dem System), Forensik, Automatisierung

Der Beitrag von GenAI zu Sicherheitstools könnte helfen, die Fähigkeiten von Sicherheitsteams zu maximieren, Kosten zu senken und die Abwehr zu verbessern. Nutzen Sie diese Lösungen, wenn sie sich weiterentwickeln und reifen.

Treiben Sie Innovationen souverän voran

Am wichtigsten ist, dass Sicherheitsrisiken Sie nicht davon abhalten sollten, potenziell revolutionäre Technologie zu nutzen. Effizienz, Automatisierung, Kostenreduzierungen, Problemlösung und die Förderung der Kreativität sind nur einige der Vorteile bei der Transformation von Unternehmen mit GenAI.

Auch wenn GenAI robuste und manchmal neue Cybersicherheitsmaßnahmen erfordert, sollte das Ziel darin bestehen, die Mission des Unternehmens zu fördern und nicht zu behindern. Die Entwicklung der richtigen Cybersicherheitsstrategie sollte Unternehmen das Vertrauen geben, zu wachsen und innovativ zu sein.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **dell.com/cybersecuritymonth**.

DELL Technologies