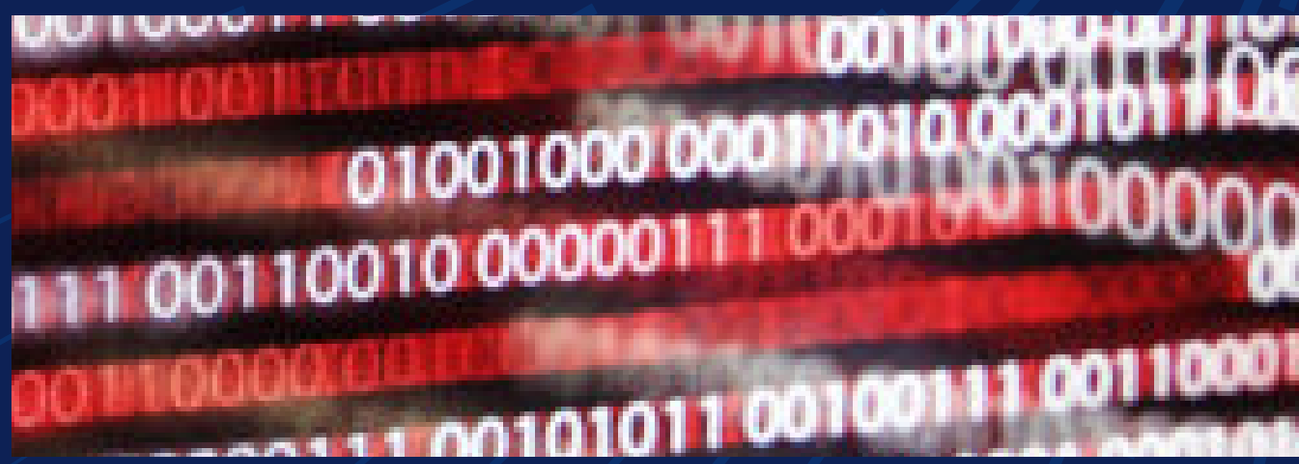
Die Cybersicherheits-Mythbusters:

Aufklären von KI-Sicherheitsmythen



KI verändert ganze Branchen, aber wenn es um die Sicherheit von KI geht, fallen viele Unternehmen Mythen zum Opfer, die sie komplexer erscheinen lassen, als sie tatsächlich ist. Die Wahrheit? Der Schutz von KI-Systemen erfordert keinen kompletten Neuanfang – die Anwendung bestehender Cybersicherheitsprinzipien auf die besonderen Herausforderungen der KI ist bereits ein großer Schritt in die richtige Richtung.

Wir bei Dell Technologies verstehen die Architektur hinter KI und können Ihnen helfen, Ihre aktuellen Lösungen an dieses neue Framework anzupassen. Lassen Sie uns die gängigsten Mythen rund um die KI-Sicherheit aufschlüsseln und die Wahrheit aufdecken, damit Sie Ihre Systeme effektiv schützen können.

Mythos 1: „KI-Systeme sind zu komplex, um sie zu schützen.“

Die Wahrheit: Es stimmt, dass KI neue Cybersicherheitsrisiken mit sich bringt, wie beispielsweise Prompt-Injection, Datenmanipulation und die Offenlegung sensibler Informationen, um nur einige zu nennen. Darüber hinaus bieten agentenbasierte KI-Systeme eine größere Angriffsfläche, da sie zur Manipulation von Ergebnissen oder zur Eskalation von Berechtigungen ausgenutzt werden können.

Allerdings ist es zwar wichtig, diese Sicherheitslücken zu erkennen und Sicherheitsmaßnahmen zu implementieren, um KI-Systeme sowohl vor herkömmlichen als auch KI-spezifischen Bedrohungen zu schützen, aber die Risiken können gemanagt und KI-Modelle gesichert werden. Es ist wichtig zu beachten, dass KI-Systeme erhebliche Datenmengen als Eingaben benötigen und große Datenmengen als Ausgaben erzeugen. Daher steht Data Protection als eine der wichtigsten Sicherheitsstrategien im Vordergrund, zusammen mit:

- Zero-Trust-Prinzipien wie Identitätsmanagement, rollenbasierter Zugriff und kontinuierliche Verifizierung.
- Regelmäßigen Penetrationstests und Sicherheitslückenmanagement zur Identifizierung von Schwächen.
- Protokollierung und Audits zur Validierung von Dateneingaben und -ausgaben

Mythos 2: „Keines meiner vorhandenen Tools wird KI sichern.“

Die Wahrheit: Bei der KI-Sicherheit geht es nicht darum, neu anzufangen, sondern darum, die bereits vorhandenen Tools intelligenter einzusetzen. Die meisten vorhandenen Cybersicherheitstools können angepasst werden, um KI-Systeme effektiv zu schützen. Im Kern ist KI eine weitere Workload in Ihrem Arsenal, die Ihr Unternehmen vorantreibt, wenn auch mit einzigartigen Eigenschaften. Grundlegende Cybersicherheitspraktiken wie Identitätsmanagement, Netzwerksegmentierung und -Monitoring, Endpunktschutz und Data Protection sind nach wie vor unerlässlich für den Schutz von KI-Umgebungen. Der Schlüssel liegt darin, diese Maßnahmen an spezifische KI-Herausforderungen anzupassen, wie z. B. den Schutz von Trainingsdaten, die Sicherung von Algorithmen und die Minderung von Risiken wie feindlichen Eingaben.

Eine starke Verteidigung beginnt mit guter Cyberhygiene, wie System-Patching, Zugriffskontrolle und Schwachstellenmanagement. Wichtig ist die Anpassung dieser Praktiken an KI-spezifische Risiken. Mit KI-fokussierten Strategien, die in Ihren aktuellen Sicherheitsansatz integriert sind, und den richtigen Tools wird KI-Sicherheit überschaubar und effektiv.

Es ist jedoch wichtig, darauf hinzuweisen, dass aktualisierte Hardware eine wichtige Rolle bei der Bekämpfung von Cyberangriffen spielen kann. Moderne KI-PCs bieten beispielsweise eine starke erste Verteidigungslinie gegen einen wichtigen Angriffsvektor: Endpunkte. Mit dem Ende des Supports für Windows 10 werden veraltete PCs zu einem Risiko. Darüber hinaus erfordert Windows 11 das Trusted Platform Module (TPM) Version 2.0, einen Sicherheitschip, der bei der Verschlüsselung, dem sicheren Start und dem Schutz vor Firmwareangriffen hilft. Viele ältere PCs verfügen entweder überhaupt nicht über TPM oder unterstützen nur eine ältere Version. Dell bietet sichere KI-PCs mit diesen integrierten Verbesserungen an.

Das Gleiche gilt für KI-Infrastruktur wie Server und Storage. Die Dell AI Factory umfasst Hardware, die für KI-Sicherheit optimiert ist und eine Reihe integrierter Sicherheitsfunktionen enthält, die von einer sicheren Lieferkette über Datenunveränderlichkeit bis hin zu Isolierung und Verschlüsselung reichen.

Mythos 3: „Bei KI-Sicherheit geht es nur darum, Daten zu schützen.“

Die Wahrheit: KI-Sicherheit geht über die grundlegende Data Protection hinaus. Sie umfasst den Schutz des gesamten KI-Ökosystems, einschließlich Modellen, APIs, Ausgaben, Systemen und Geräten. Wenn KI zunehmend in kritische Anwendungen integriert wird, eskalieren die Risiken, die mit ihrer missbräuchlichen Nutzung oder Ausbeutung verbunden sind. Ohne robuste Sicherheitsmaßnahmen können KI-Modelle manipuliert werden, um schädliche oder irreführende Ergebnisse zu generieren. APIs können ausgenutzt werden, um unbefugten Zugriff auf sensible Systeme zu erhalten, und Ausgaben können unbeabsichtigt private oder vertrauliche Informationen offenlegen.

Umfassende KI-Sicherheit erfordert einen mehrschichtigen Ansatz. Dazu gehören der Schutz von Modellen vor Angriffen, die versuchen, Eingabedaten zu manipulieren, um KI-Systeme zu täuschen, die Sicherung von APIs mit starken Authentifizierungsmethoden, um unbefugte Nutzung zu verhindern, und das **kontinuierliche Monitoring von Ausgaben** auf ungewöhnliche oder verdächtige Muster, die auf einen Angriff oder eine Fehlfunktion hindeuten könnten. Eine effektive KI-Sicherheit sorgt nicht nur für die Integrität und Zuverlässigkeit von KI-Systemen, sondern schafft auch Vertrauen bei NutzerInnen und StakeholderInnen, indem sie die Risiken bösartiger Nutzung oder unbeabsichtigter Folgen mindert.

Mythos 4: „KI benötigt keine menschliche Aufsicht."

Die Wahrheit: Governance und menschliche Aufsicht sind entscheidend, um sicherzustellen, dass KI-Systeme ethisch, vorhersehbar und in Übereinstimmung mit den menschlichen Werten funktionieren. Fortschrittliche KI-Systeme, insbesondere agentenbasierte KI mit autonomen Entscheidungsfähigkeiten, bringen einzigartige Herausforderungen mit sich, die robuste Sicherheitsvorkehrungen erfordern. Ohne angemessene Überwachung können diese Systeme von den beabsichtigten Zielen abweichen oder unbeabsichtigte Verhaltensweisen aufweisen, die Risiken darstellen.

Um dies zu erreichen, ist es unerlässlich, klare Grenzen zu schaffen, mehrschichtige Kontrollmechanismen zu implementieren und sicherzustellen, dass Menschen kontinuierlich in kritische Entscheidungsprozesse einbezogen werden. Regelmäßige Audits, Transparenz bei KI-Prozessen und gründliche Tests können die Verantwortlichkeit und das Vertrauen weiter stärken, wodurch Missbrauch verhindert und der verantwortungsvolle Einsatz von KI-Technologien gefördert wird.

Best Practices zur Stärkung der KI-Sicherheit

Um KI-spezifische Sicherheitslücken zu schließen, müssen Unternehmen einen proaktiven und strategischen Ansatz verfolgen. Hier sind 10 Empfehlungen zur Sicherung Ihrer KI-Systeme:

Mehrschichtige Sicherheitsarchitektur:
Nutzen Sie Segmentierung, Firewalls und starke Authentifizierung, um Ihre Infrastruktur, Software und Daten auf jeder Ebene zu schützen.

Sicherung der Lieferkette:
Implementierung eines starken Lieferantenmanagementprogramms. Prüfen Sie Anbieter und Komponenten von Drittanbietern, validieren Sie die Integrität und verlassen Sie sich auf signierten Code, um Schwachstellen im KI-Entwicklungszyklus zu vermeiden.

Schutz von Trainingsdaten und -Modellen:
Schützen Sie sich vor verunreinigten Daten, feindliche Eingaben und anderen Bedrohungen, indem Sie die Datenintegrität überwachen und robuste Validierungstools anwenden.

Verschärfen der Zugriffskontrollen:
Setzen Sie das Least-Privilege-Prinzip durch, implementieren Sie rollenbasierte Zugriffskontrollen (RBAC), wechseln Sie regelmäßig die Anmeldedaten und überprüfen Sie die Berechtigungen, um unbefugten Zugriff zu verhindern.

Sichere APIs:
Verwenden Sie strenge Authentifizierungsprotokolle (wie OAuth 2.0), erzwingen Sie die HTTPS-Verschlüsselung und aktualisieren Sie APIs regelmäßig, um potenzielle Sicherheitslücken zu schließen.

Überwachen und Validieren von KI-Ausgaben:
Verwenden Sie Anomalieerkennung, Protokollierung und Warnmeldungen, um ungewöhnliche Muster oder schädliche Verhaltensweisen in KI-Ergebnissen zu überwachen.

Planen für Resilienz:
Sie sollten Ihre Daten regelmäßig sichern und Disaster-Recovery-Pläne testen, um Ausfallzeiten zu minimieren und eine schnelle Wiederherstellung im Falle einer Sicherheitsverletzung sicherzustellen.

Implementieren einer zuverlässigen Verschlüsselung:
Verschlüsseln Sie sensible Daten im Ruhezustand und während der Übertragung mithilfe starker Algorithmen und verwalten und rotieren Sie Verschlüsselungsschlüssel regelmäßig und sicher.

Durchführung regelmäßiger Sicherheitsaudits und Penetrationstests:
Überprüfen Sie Systeme regelmäßig auf Schwachstellen und nutzen Sie Penetrationstests, um Risiken aufzudecken, bevor sie ausgenutzt werden können.

Schulung von MitarbeiterInnen zu Best Practices für KI-Sicherheit:
Schulen Sie Ihr Team regelmäßig in Bezug auf sichere Entwicklung, Bedrohungserkennung und die Aufrechterhaltung strenger Sicherheitspraktiken, um Sicherheitsverletzungen zu verhindern.

DELL Technologies

Das Wertversprechen von Dell: praktische KI-Sicherheitslösungen.

KI-Sicherheit mag komplex erscheinen, ist aber nicht so erschreckend, wie sie scheint. Die Wahrheit? KI-Sicherung unterscheidet sich nicht so sehr von der Sicherung vorhandener Workloads – es geht darum, die Architektur zu verstehen und die richtigen Strategien anzuwenden. Hier kommt Dell Technologies ins Spiel.

Wir entmystifizieren KI-Sicherheit, indem wir Ihre aktuellen Lösungen nutzen und sie nahtlos in KI-fokussierte Architekturen integrieren. Wir bewältigen Herausforderungen wie Prompt-Injection, API-Missbrauch und gegnerische Angriffe, ohne dass eine komplette Überarbeitung der Infrastruktur erforderlich ist.
Die Expertise von Dell liegt darin, mit den Mythen rund um KI-Sicherheit aufzuräumen und zu zeigen, wie realisierbar sie tatsächlich ist. Ganz gleich, ob Sie gerade erst mit KI beginnen oder Ihre Abwehrmaßnahmen verbessern möchten, wir helfen Ihnen dabei, Ihre Investitionen zu schützen, Ihre Systeme zu sichern und eine resiliente digitale Zukunft aufzubauen – souverän und effektiv. Vereinfachen wir gemeinsam die KI-Sicherheit.

Dell Produkte und Lösungen für Ihre Unterstützung

Empfohlene Dell Lösung	Beschreibung
Dell AI Factory	Dell AI Factory sichert KI-Workloads über eine sichere Lieferkette und gewährleistet eine vertrauenswürdige Infrastruktur von der Entwicklung bis zur Bereitstellung. Mit Funktionen wie Datenunveränderlichkeit, Isolierung und Verschlüsselung schützt sie sensible Modelle und Datenvolumen, wehrt Cyberbedrohungen ab und ermöglicht skalierbare, effiziente und nahtlose KI-Operationen in dynamischen, datengesteuerten Umgebungen.
Ausfallsicherheit bei Cyberangriffen	PowerProtect schützt KI-Workloads mit erweiterten Funktionen wie Unveränderlichkeit und Isolierung und gewährleistet so Datenintegrität und Schutz vor Cyberbedrohungen. Die Lösung bietet End-to-End-Verschlüsselung und Anomalieerkennung und ermöglicht gleichzeitig eine schnelle Recovery, um Ausfallzeiten zu minimieren.
Dell Trusted Workspace (Endpunktsicherheit)	Eine Kombination aus integrierten und optionalen Zusatzfunktionen, die zur Sicherung von KI-PCs und der darauf ausgeführten KI-Workloads entwickelt wurden. Die integrierten Funktionen basieren auf sicheren Lieferkettenpraktiken und umfassen SafeBIOS und SafeID mit TPM. Zu den optionalen Zusatzfunktionen gehören Secured Component Verification, SafeID mit ControlVault sowie die Partnersoftware CrowdStrike und Absolute, um die Sicherheit am Arbeitsplatz zu maximieren.
KI-Sicherheitsempfehlungs-services	Eine Suite von Services, die Sie bei der Entwicklung und Implementierung einer umfassenden KI-Sicherheitsstrategie unterstützen können. Das Angebot umfasst Beratungsdienste, KI-vCISO und Datensicherheitsplanung.
Managed Security Operations für KI	Ermöglicht umfassende Transparenz im gesamten Stack, um Bedrohungen schnell zu erkennen und auf sie zu reagieren. Zu den Funktionen gehören Managed Detection and Response, Managed AI Guard, Penetrationstests für KI sowie Incident Response and Recovery Services.
Integration von Sicherheitssoftware	Entwerfen, installieren und konfigurieren Sie Sicherheitstools, die Zugriffsmanagement, Anwendungen, Netzwerke, Clouds und mehr schützen.

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