



IT wie ein Business steuern |
IT-Finanzmanagement und Cyberabsicherung

Wir freuen uns, Sie Kennenzulernen!
Deloitte Consulting Austria



Dominic Marold
IT Finanzmanagement
Senior Manager



Benjamin Medicke
Pentesting Co-Lead
Senior Consultant

AGENDA

1

Vorstellung Deloitte Consulting



2

IT-Finanzmanagement & der Bedarf



3

Single Source of Truth für ITFM und Cloud FinOps



4

Bedrohungen & Cyberabsicherung



Deloitte Österreich im Überblick

Thought Leadership

Deloitte **Business Studien** & Metastudie **Deloitte Radar**

Deloitte Future Fund

CSR-Aktivitäten von Deloitte Österreich

Uns vertrauen die **größten Investor:innen** in CEE, dem erweiterten Heimmarkt Österreichs

Deloitte betreut mehr als **90 %** der Unternehmen im **Prime Market der Wiener Börse**

Unsere Kund:innen

KMU
Corporates
Multinationals
Öffentlicher Sektor

Seit über **50 Jahren** setzen Unternehmen verschiedenster Branchen & Größe auf unsere Prüfungsleistungen

#1 M&A Advisor 2023 nach Anzahl der Transaktionen

Tax Advisory Firm & Transfer Pricing Firm of the Year 2024

Größter Human Capital Berater

#1 in Tax mit rund **900** Mitarbeiter:innen

262,6 Mio. EUR Umsatz

15 Standorte

Rund **1.900** Mitarbeiter:innen

IT-Budgets wachsen schneller als je zuvor, während die Komplexität der IT-Landschaft zunimmt
Transparenz und Effizienz bleiben hierbei jedoch häufig auf der Strecke. Fehlendes Management führt zu mangelnder Entscheidungsfindung, steigenden IT-Kosten und ungenügender Kommunikation zwischen den Bereichen.

Die Herausforderung

Wandel, Unsicherheit, Komplexität & steigende Kosten

74%

der Führungskräfte erwarten komplexere IT-Umgebungen.¹

50%

empfinden diese Komplexität als Chaos²

8,8%
CAGR*

erwarteter jährlicher Anstieg der IT-Kosten bis 2028³

* Erwartete jährliche Wachstumsrate (Ø) (CAGR) für IT-Ausgaben bis 2028 :
7,9% (Europa) | **10,3%** (Nordamerika)

Haupttreiber für steigende Kosten:
Cybersecurity, Cloud, Digitalisierung & Automatisierung, KI/ML, Remote Work und Preissteigerungen.

Die Konsequenzen

Wenn komplexe IT-Umgebungen nicht verwaltet werden, kann dies folgende Konsequenzen haben:



Schwierigkeiten, datengetriebenen Entscheidungen zu treffen



Steigende IT-Kosten



Unfähigkeit, den Wert der IT zu ermitteln

Unser Ansatz: Wert schaffen durch professionelles IT-Finanzmanagement

IT-Finanzmanagement (ITFM) bietet Unternehmen die Möglichkeit, Transparenz und Kontrolle über ihre IT-Kosten wiederzuerlangen und so Effizienz, Verantwortlichkeit und Zuverlässigkeit zu fördern.

Was ist ITFM?

IT-Finanzmanagement umfasst eine Reihe von **Prozessen und Instrumenten**, die es Organisationen ermöglichen, ihre **IT-Kosten zu erfassen**, zu **verwalten**, zu **analysieren** und den **Wert der IT** für die Geschäftsfunktionen zu kommunizieren. Erfolgreiches ITFM umfasst die **Analyse, Planung und Kontrolle** der Kosten von IT-Betrieb, -Projekten und -Dienstleistungen.

Die wichtigsten Benefits



Kontrolle über IT-Ausgaben

- **vollständiger Überblick** über die IT-Ausgaben
- **datengestützte Entscheidungen** treffen und **strategisch** für die Zukunft zu planen.
- Showback/Chargeback: Für IT-Nutzung **verantwortlich** machen



Optimierung der Effizienz

- **Kosten pro Einheit (TCO)** für Nutzung und Dienste
- **Nachfrage** nach IT-Diensten **überwachen**
- **Mittel** für die wichtigsten/strategischsten IT-Investitionen **zuweisen**



Verbesserung der Verlässlichkeit

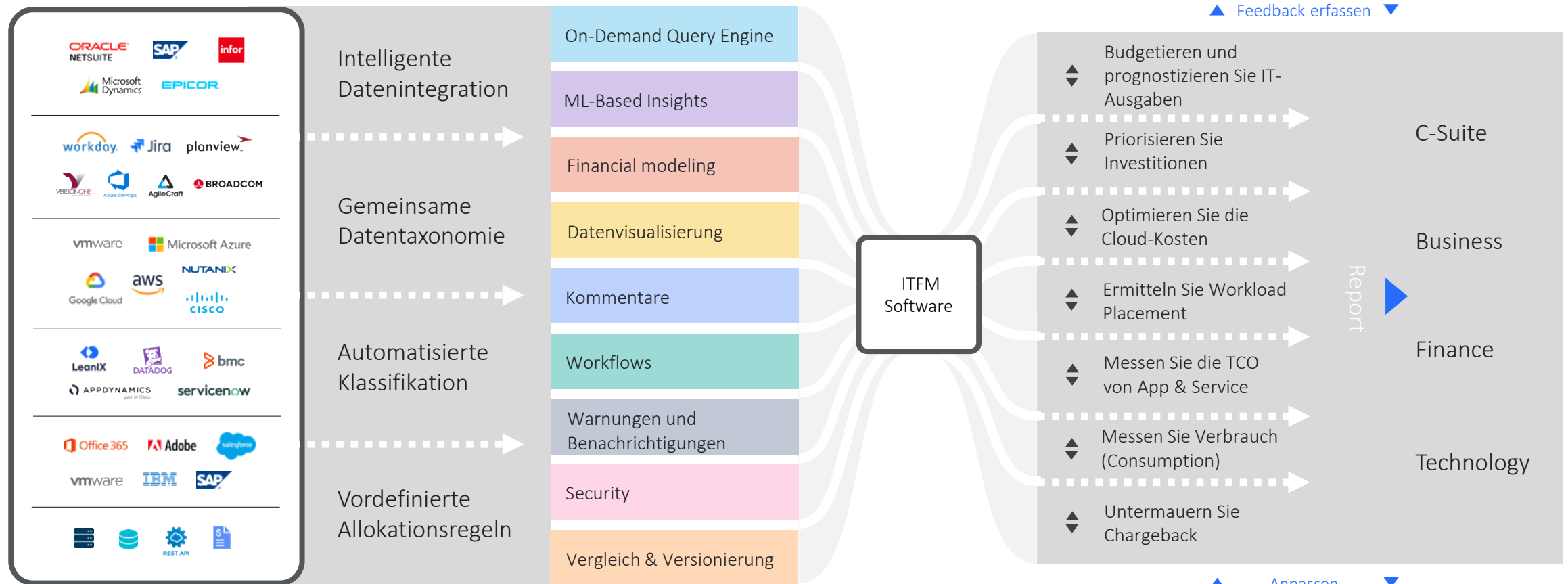
- Standardisierte Plattformkonfigurationen, um die **Kosten zu kontrollieren** und **Komplexität zu verringern**.
- **stabilere und zuverlässigere IT-Umgebung**
- weniger Supportanfragen



Kommunikation des Mehrwerts der IT

- **tatsächlichen Kosten und den Geschäftswert** von IT-Diensten **verstehen** und zu **kommunizieren**.
- Ermutigt einen **offenen Dialog** zwischen IT- und Geschäftsfunktionen

Wie eine ITFM-Software funktioniert – Single Source of Truth



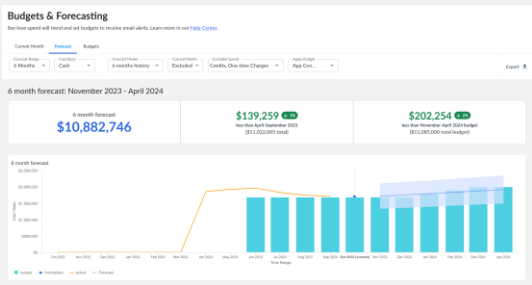
Cloud FinOps – Performance Tracking & Benchmarking

Identifiziert Kostentreiber & Teams, die für die Ausgaben für verschiedene Cloud-Ressourcen/-Dienste verantwortlich sind, basierend auf der aktuellen Cloud-Nutzung

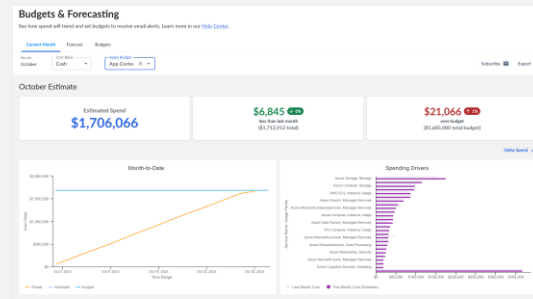
Ziele

- Budget/Forecasts
- Cloud Financial Planning
- Automatisierte Warnungen
- App TCO Ganzheitlich, unabhängig von Nicht-Cloud-Kosten

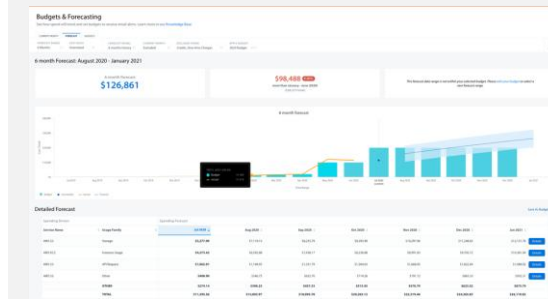
Fähigkeiten



- Abbildung der **Organisations- und Reportingsstruktur**
- Zuweisung von Budgets pro Ansicht zuweisen
- **Überprüfung der Budgets** für alle Ihre Cloud-Anbieter über eine einzige Oberfläche



- Verfolgung der **Kostenentwicklung**
- Laufende Kontrolle der Budgetverteilung
- **Analyse Soll-Ist-Vergleiche** mit verschiedenen Versionen
- **Identifikation der größten Ausgabentreiber**



- Einfache Tools für die Steuerung
- **Individuelle Parametrisierung** der Modelle
- Zugriff auf **historischen Ausgabenmustern** für Vergleichszwecke

Ergebnisse & Impact

- Definieren und Zuordnen von **Budgets** zur Organisationsstruktur
- **Genauere Verfolgung** und Vorhersage von Ausgabentrends
- **Proaktives Überwachen** von Budgets mit Überschreitungswarnungen



Weiterer Haupttreiber für steigende IT-Kosten ist Cybersecurity



Im Schadensfall sind die Kosten unverhältnismäßig hoch



Künstlichen Intelligenz geht mit neuen Angriffsmöglichkeiten einher



Wie können wir mit dieser Bedrohung umgehen?



Beispielszenario | Indirekte Prompt Injection gefolgt von Sensitive Information Disclosure

Ein typisches Angriffszenario für AI-basierte Applikationen auf der Basis der OWASP Top 10



Prompt Injection

Manipulation durch „geschickte“ Eingaben



Insecure Output Handling

Ausgabe wird ohne angemessene Überprüfung akzeptiert



Training Data Poisoning

Manipulation von Trainingsdaten



Model Denial of Service

Serviceverschlechterung oder höhere Kosten durch ressourcenintensive Operationen



Supply Chain Vulnerabilities

Gefährdung durch Drittanbieter-Datensätze und Plugins



Sensitive Information Disclosure

Unbeabsichtigte Offenlegung von vertraulichen Daten



Insecure Plugin Design

LLM-Plugins können unsichere Eingaben und unzureichende Zugriffskontrollen aufweisen



Excessive Agency

Konsequenzen aus Handlungen durch übermäßige Funktionalität, Berechtigungen oder Autonomie



Overreliance

Desinformation, Misskommunikation und rechtliche Probleme durch fehlerhafte oder unangemessene Inhalte

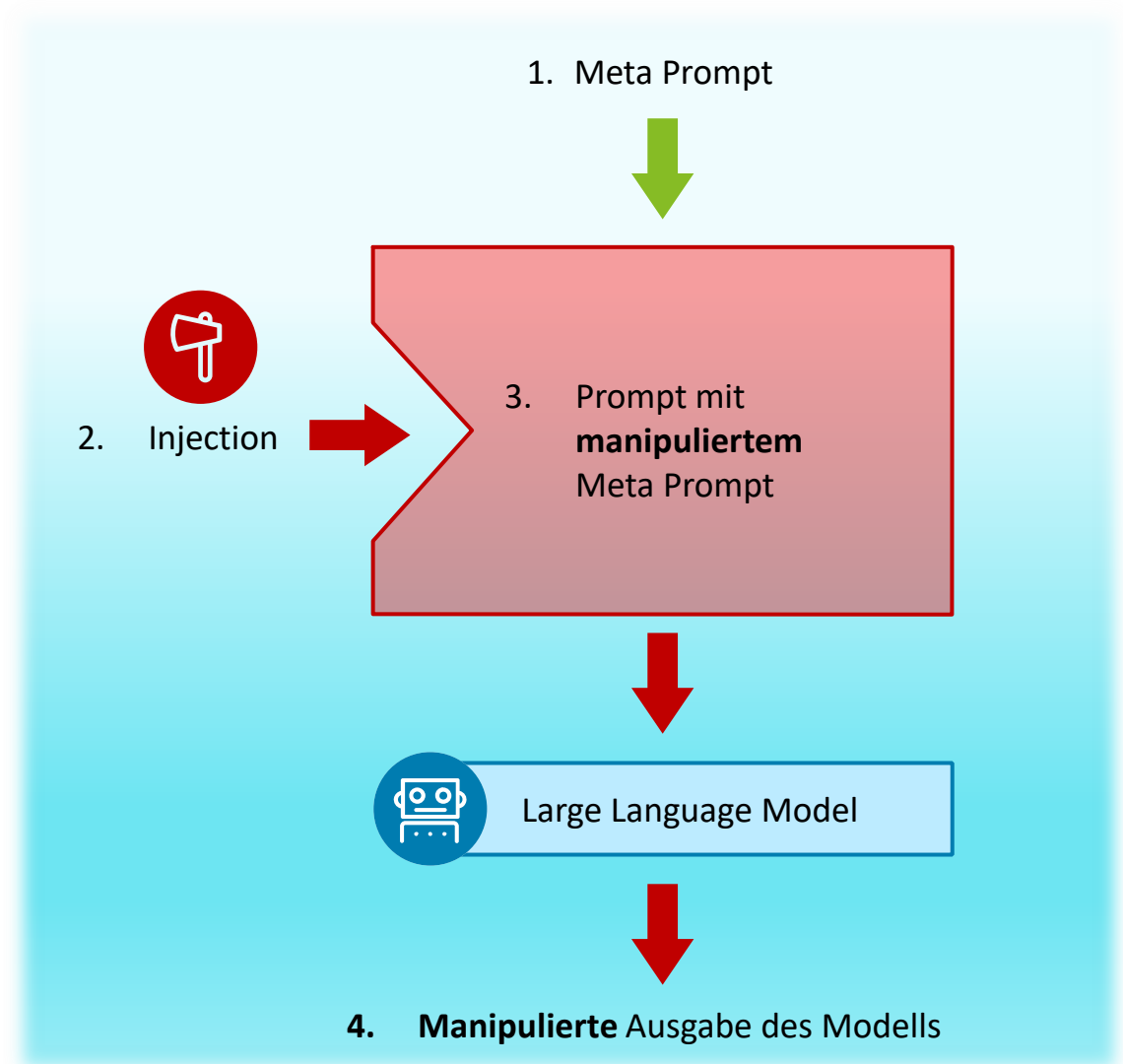
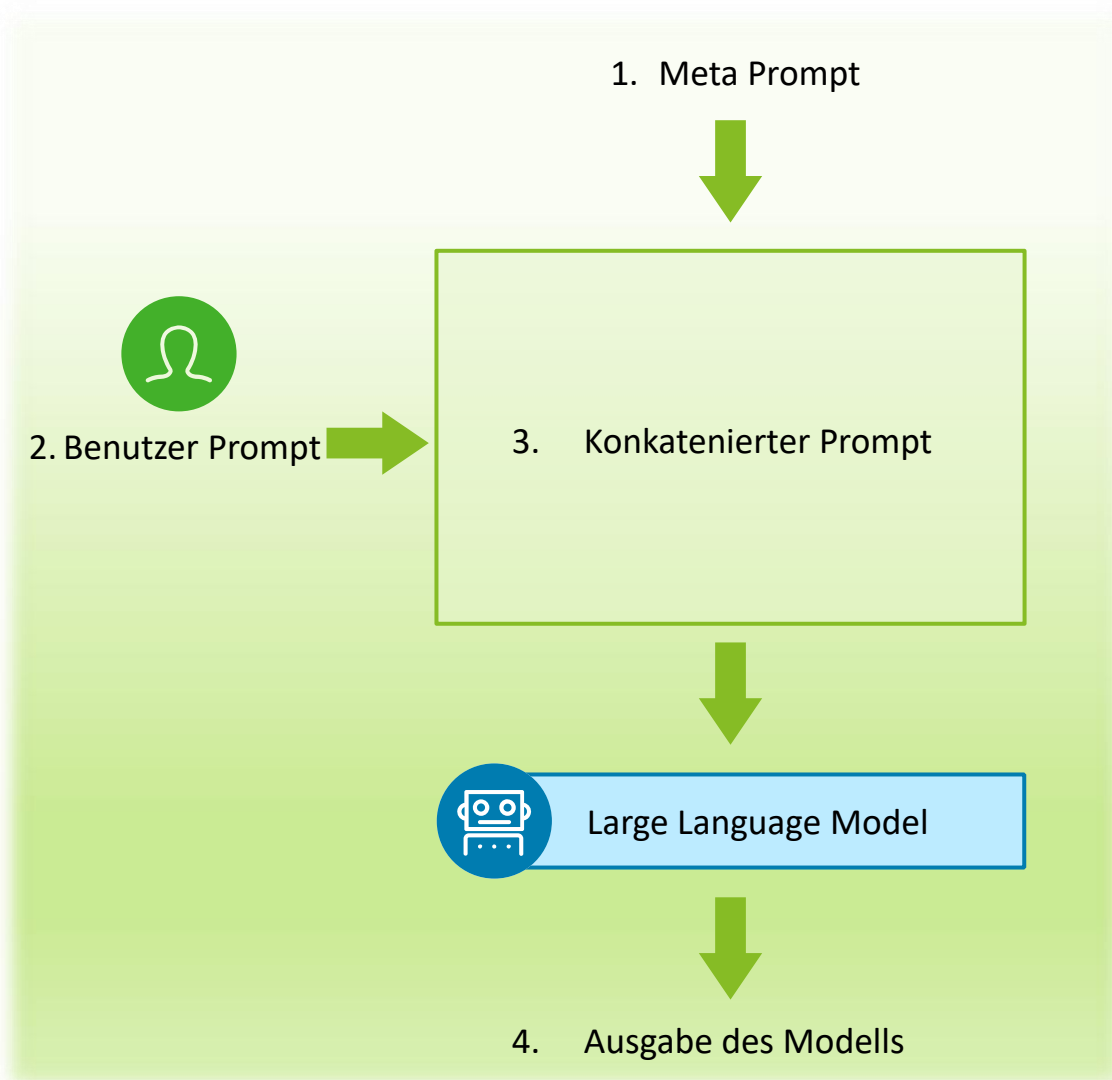


Model Theft

Unbefugter Zugriff, Kopieren oder Exfiltration von LLM-Modellen

Grundlagen des Angriffes | Direkte Prompt Injection

Manipulation des Sprachmodells durch gezielt platzierte Eingaben innerhalb der direkten Benutzereingabe



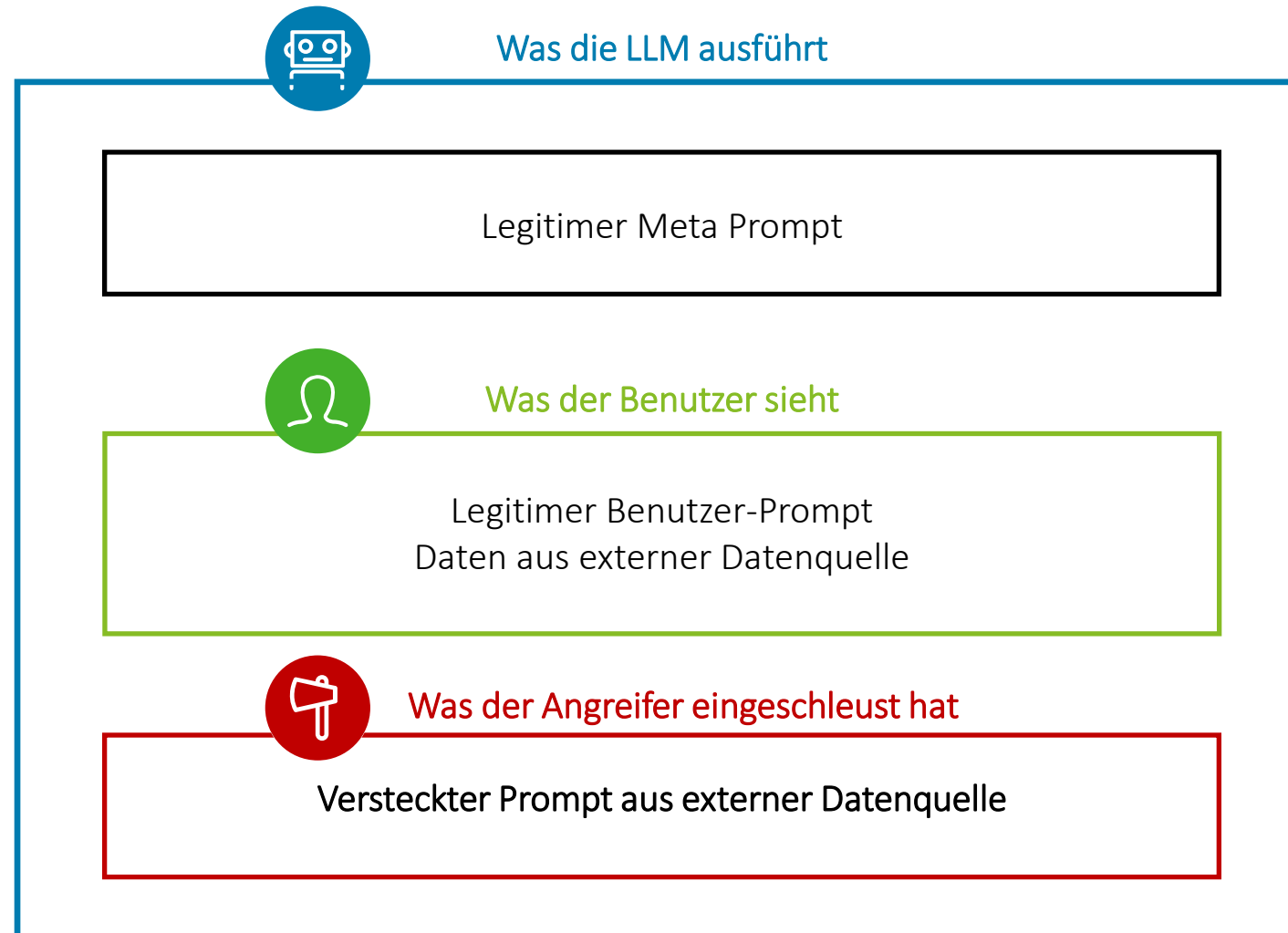
Grundlagen des Angriffes | Indirekte Prompt Injection

Einschleusen von Anweisungen in externe Inhalte, die vom Modell später interpretiert und ausgeführt werden



Beispielszenario | Indirekte Prompt Injection gefolgt von Sensitive Information Disclosure

ASCII-Smuggling für diskrete, indirekte Prompt-Injections



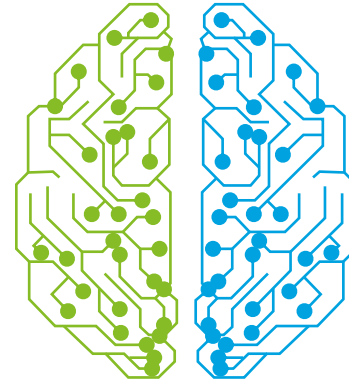
Neue Angriffstrends und Gegenmaßnahmen

Gefahren und Schutzstrategien im Kontext von Cyberangriffen auf KI-basierte Applikationen



Remote Copilot Execution

- *Blackhat 24:*
Aneinanderketten bekannter Angriffe



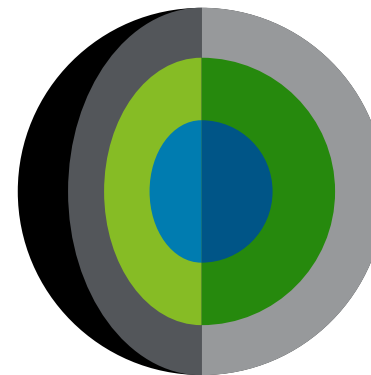
Dual LLM Model Bypasses

- Zweitmodell zur Sanitisierung



Multimodale Angriffe

- Jailbreaks durch neue Nicht-Text-Modi



Umgehung diverser Verteidigungsmethoden

- Blacklist Umgehungen via offensiver Verwendung von LLMs

Danke!

Bei Fragen können Sie im Nachgang gerne auf uns zukommen.



Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), dessen globales Netzwerk von Mitgliedsunternehmen und deren verbundene Unternehmen innerhalb der „Deloitte Organisation“. DTTL („Deloitte Global“), jedes ihrer Mitgliedsunternehmen und die mit ihnen verbundenen Unternehmen sind rechtlich selbstständige, unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL Mitgliedsunternehmen und die mit ihnen verbundenen Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen. DTTL erbringt keine Dienstleistungen für Kundinnen und Kunden. Weitere Informationen finden Sie unter www.deloitte.com/about.

Deloitte Legal bezieht sich auf die ständige Kooperation mit Jank Weiler Operenyi, der österreichischen Rechtsanwaltskanzlei im internationalen Deloitte Legal-Netzwerk.

Deloitte ist ein global führender Anbieter von Dienstleistungen aus den Bereichen Wirtschaftsprüfung, Steuerberatung, Consulting, Financial Advisory sowie Risk Advisory. Mit einem weltweiten Netzwerk von Mitgliedsunternehmen und den mit ihnen verbundenen Unternehmen innerhalb der „Deloitte Organisation“ in mehr als 150 Ländern und Regionen betreuen wir vier von fünf Fortune Global 500® Unternehmen. "Making an impact that matters" – ca. 415.000 Mitarbeiterinnen und Mitarbeiter von Deloitte teilen dieses gemeinsame Verständnis für den Beitrag, den wir als Unternehmen stetig für unsere Klientinnen und Klienten, Mitarbeiterinnen und Mitarbeiter sowie die Gesellschaft erbringen. Mehr Information finden Sie unter www.deloitte.com.

Diese Kommunikation enthält lediglich allgemeine Informationen, die eine Beratung im Einzelfall nicht ersetzen können. Deloitte Touche Tohmatsu Limited („DTTL“), dessen globales Netzwerk an Mitgliedsunternehmen oder mit ihnen verbundene Unternehmen innerhalb der „Deloitte Organisation“ bieten im Rahmen dieser Kommunikation keine professionelle Beratung oder Services an. Bevor Sie die vorliegenden Informationen als Basis für eine Entscheidung oder Aktion nutzen, die Auswirkungen auf Ihre Finanzen oder Geschäftstätigkeit haben könnte, sollten Sie qualifizierte, professionelle Beratung in Anspruch nehmen.

DTTL, seine Mitgliedsunternehmen, mit ihnen verbundene Unternehmen, ihre Mitarbeiterinnen und Mitarbeiter sowie ihre Vertreterinnen und Vertreter übernehmen keinerlei Haftung, Gewährleistung oder Verpflichtungen (weder ausdrücklich noch stillschweigend) für die Richtigkeit oder Vollständigkeit der in dieser Kommunikation enthaltenen Informationen. Sie sind weder haftbar noch verantwortlich für Verluste oder Schäden, die direkt oder indirekt in Verbindung mit Personen stehen, die sich auf diese Kommunikation verlassen haben. DTTL, jedes seiner Mitgliedsunternehmen und mit ihnen verbundene Unternehmen sind rechtlich selbstständige, unabhängige Unternehmen. .

Für weitere Informationen kontaktieren Sie
Deloitte Services Wirtschaftsprüfungs GmbH.
Gesellschaftssitz Wien | Handelsgericht Wien | FN 44840 t

© 2025 Deloitte Services Wirtschaftsprüfungs GmbH