



Identity Management im Zeitalter von KI



Fabian Böhm

CEO & Founder von TEAL

 <https://www.teal-consulting.de/>

 [LinkedIn](#)



IdentityProtection

Architecture

TEAL
ALWAYS CHALLENGING IT

Hollywood lügt uns seit Jahren an...



Über (2022)

Der Angreifer bombardierte einen Mitarbeiter mit MFA-Anfragen, bis dieser eine bestätigte ("MFA Fatigue"). Anschließend konnte sich der Angreifer mit legitimen Rechten bewegen.

Quelle: [Security update](#)

Passwort des Exchange Service Accounts im Beschreibungsfeld. Wurde erst nach 5 Jahren bei einem Test zufällig entdeckt.

Jetzt kommt KI ins Spiel.

“

*KI IST DER NEUE TURBO
FÜR HACKER.*

*IDENTITÄTSSCHUTZ IST DIE
EINZIGE BREMSE, DIE
NOCH FUNKTIONIERT.*

VOM HACKEN ZUM EINLOGGEN

Moderne Angreifer nutzen KI nicht nur für komplexe Code-Exploits, sondern um **valide Identitäten** zu stehlen.



Hyper-Personalisierung:

Phishing-Mails, die nicht mehr von echten Mails unterscheidbar sind.



Adaptive Malware:

Schädlinge, die Sicherheitssoftware in Echtzeit umgehen.



Mass-Credential Stuffing:

KI-gestütztes Knacken von Pattern-basierten Passwörtern.



MFA bypass:

Echtzeit-Diebstahl von Logins hebt Mehrfaktor-Schutz aus.



Social Engineering perfektioniert:

KI-Stimmenimitation und Deepfakes machen Täuschungen unsichtbar.

Verteidiger brauchen KI

Alle suchen den **Einbruch.**



Niemand sucht die **Berechtigung**

TEAL
Das IT-Unternehmen

Menschen können die Geschwindigkeit der Angreifer nicht mehr allein ausgleichen.

- Mehr Signale
- Mehr Anmeldungen
- Mehr Anomalien
- KI zur Risikoerkennung und Priorisierung

"Wenn Angreifer mit KI arbeiten und Verteidiger nicht, entsteht ein unfaires Rennen."

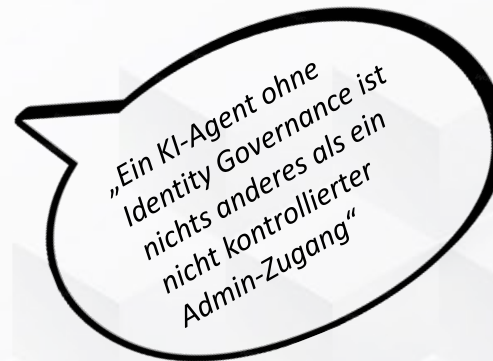
KI-Agenten sind die neuen Benutzer in deiner Umgebung

Realität

- KI-Agenten kennen Dokumente, Mails, Chats und Prozesse
- Oft überprivilegiert
- Vielleicht fragt der Angreifer künftig nicht mehr das System, vielleicht fragt er den Agenten

Risiko

- Überprivilegierte Zugriffe
- Fehlende Zugriffskontrolle
- keine Identitätstrennung
- schwer auditierbar



Fazit: Die wichtigste Frage bleibt dieselbe - Wer darf worauf zugreifen?

- KI beschleunigt Angriffe
- KI beschleunigt Verteidigung
- Berechtigungen entscheiden über den Schaden
- Das gilt für Benutzer genauso wie für KI-Agenten

"KI verändert die Geschwindigkeit des Spiels. Gewonnen wird aber immer noch über Identitäten und Berechtigungen. Wer beides im Griff hat, hat auch gegen KI-gestützte Angreifer eine Chance."

Danke



E-Mail: fabian.boehm@teal-consulting.de

Security Newsletter:
<https://www.teal-consulting.de/newsletter/>

