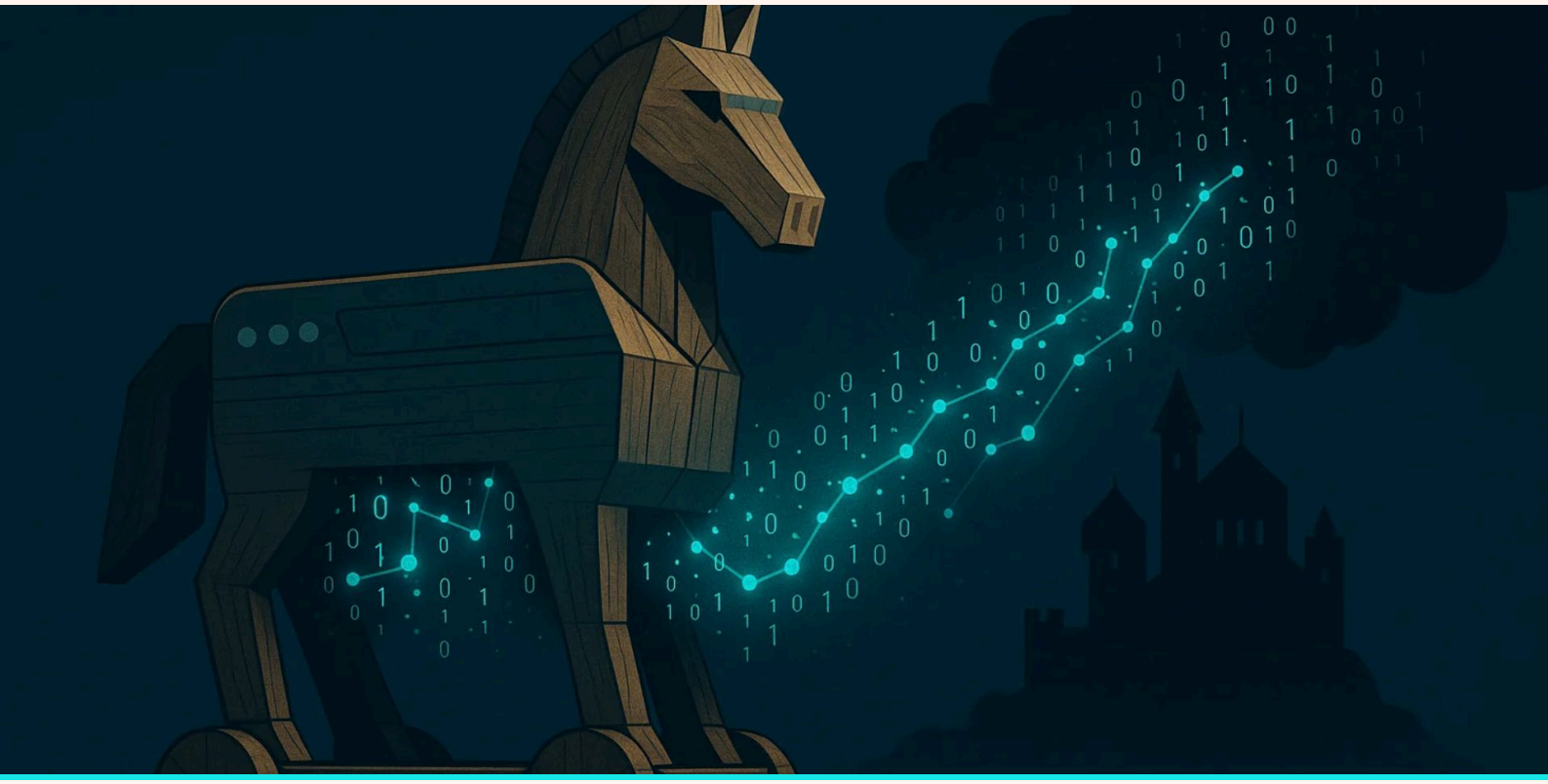
Tech Industry Leadership
KI, Automatisierung und Führung



KI-Sicherheit im Unternehmen:

KI-Browser sind die neuen Trojaner

– nur dass du sie selbst installiert hast.

Neue KI-Browser versprechen eine Revolution im Arbeitsalltag, doch sie greifen in alles hinein, was du im Browser tust – und sind laut aktuellen Analysen bis zu 85 % leichter zu hacken. Welche Alternativen es gibt und was du heute noch tun solltest, erfährst du in diesem Newsletter.

Warum du KI-Browser derzeit nicht in deinem Unternehmen einsetzen solltest und welche Alternativen es gibt

Die neue Versuchung am digitalen Arbeitsplatz

Vielleicht hast du schon davon gehört: neue „KI-Browser" wie **Comet** von *Perplexity* oder Microsofts **Copilot-Browser-Integrationen** versprechen eine Revolution im Arbeitsalltag.
Sie recherchieren für dich, schreiben Mails, fassen Webseiten zusammen, beantworten Fragen im Kontext deiner Tabs – und das alles direkt im Browser.

Klingt großartig, oder?
Ist es. Aber es ist eben auch brandgefährlich.

Denn diese Tools greifen in alles hinein, was du im Browser tust – Mails, CRM, Cloud-Dokumente, Formulare, Logins, Bezahlseiten.
Und **genau dort**, an der Schnittstelle zwischen Komfort und Kontrolle, beginnt das Problem.

„Wir testen nur kurz…“ – und öffnen damit alle Türen

Ein Kunde aus der Fertigungsindustrie erzählte mir kürzlich stolz, sein Team habe Comet „einfach mal ausprobiert“.
Ein paar Wochen später war klar:
Die Mitarbeiter hatten mit der KI nicht nur Webseiten analysiert, sondern unbewusst auch interne Preislisten, Lieferantennamen und Vertragsnummern übermittelt – an Server, deren Hosting-Ort niemand prüfen konnte.

Kein böser Wille, keine Schlamperei.
Nur ein typisches Beispiel für die **Schattennutzung neuer Tools** – und für den massiven Kontrollverlust, der entstehen kann, wenn man solche Technologien unvorbereitet einsetzt.

Was gerade passiert: ein Markt explodiert – und mit ihm das Risiko

Die Zahlen sind beeindruckend:
Der Markt für KI-Browser soll laut aktuellen Prognosen von **4,5 Mrd. USD (2024)** auf **77 Mrd. USD (2034)** wachsen – das sind unglaubliche **33 % Wachstum pro Jahr**.
Interessanterweise sollen **76 %** dieser Nutzung im Unternehmenskontext stattfinden, wo Sicherheit und Datenschutz eigentlich unumgänglich sein sollten.

Aber: Laut mehreren aktuellen Analysen sind KI-Browser derzeit **bis zu 85 % leichter zu hacken** als herkömmliche Browser, weil sie neue, bislang ungeschützte Angriffsflächen öffnen.

Übersicht mit den derzeit wichtigsten fünf KI-Browsern

Comet von Perplexity AI

Microsoft Edge (Copilot Mode) von Microsoft

Opera One / **Opera Neon** (mit Aria) von Opera Software ASA

Dia Browser von The Browser Company

Sigma AI Browser von Sigma Labs Inc.

Und was ist mit Microsoft Copilot?

Copilot ist im Vergleich zu Comet deutlich strukturierter aufgebaut – mit Audit-Logs, Datenklassifizierung und Enterprise Data Protection.
Aber auch hier gilt: **Nur so sicher wie seine Konfiguration.**
Wer ohne Governance, Rollenrechte und klare Prompt-Policies startet, riskiert denselben Kontrollverlust – nur eleganter verpackt.

Zugang zur „Tiefe“ der Unternehmensdaten

Copilot greift zudem auf interne Datenquellen via Graph zu – das ist leistungsstark, aber gleichzeitig eine Schwachstelle. Ein KI-Browser kann bewusst nur eine Teilmenge von Daten nutzen, wenn du ihn entsprechend beschränkst: z. B. nur auf ausgewählte Wiki-Einträge, nicht auf E-Mails, Projekt-Datenbanken.

Bei Copilot ist der Zugang tiefer und damit riskanter – das heißt: du bekommst zwar potenziell bessere Ergebnisse, aber auch ein höheres Risiko.
Kurz: Der Vorteil (tieferer Datenzugriff) ist gleichzeitig ein Nachteil – weil mehr Angriffsfläche.

Selbst bei sorgfältiger Vorbereitung und initialer Konfiguration bleiben also bestimmte Risiken bestehen.

Risiken am Beispiel von Copilot:

a) Über- bzw. Fehlberechtigungen bleiben ein Risiko

Auch wenn Rollen- und Rechtekonzepte vorhanden sind: Studien zeigen, dass in Unternehmensumgebungen oft **95 % der Berechtigungen nicht genutzt** werden – aber dennoch bestehen. Wenn diese ungenutzten Berechtigungen mit der Zugriffstiefe von Copilot kombiniert werden, entsteht folgendes Szenario:

Copilot greift auf alle Daten zu, die der Nutzer sehen darf („least privilege“ wurde umgesetzt). Das heißt: Ein Prompt könnte Daten zusammenführen, die zwar einzeln erlaubt sind, aber zusammen eine sensible Informationseinheit ergeben (z. B. Preislisten + Lieferantenliste + Vertragsbedingung). Selbst bei „korrekten“ Policies bleibt das Risiko, dass alte, vergessene oder wenig überwachte Datenquelle („Archive“, SharePoint-Sites, Teams-Kanäle) von Copilot genutzt werden und so intern mehr geteilt wird als gewollt.

b) Artefakt- und Persistenzrisiken

Mit dem Einsatz von Copilot entstehen neue „Artefakte“: das sind nicht nur generierte Antworten, sondern auch andere Inhalte – Protokolle, Zwischenergebnisse, Referenzen.

Diese Artefakte unterliegen denselben rechtlichen Anforderungen wie andere Informationen (z. B. eDiscovery, Datenaufbewahrung, Löschfristen). Wenn nicht sauber gesteuert, kann generierter Inhalt viel länger oder anders gespeichert werden als erwartet – Risiko für Compliance-Verstöße. Darüber hinaus: Kopien oder Referenzen dieser Inhalte könnten außerhalb kontrollierter Umgebungen landen, wenn Nutzer sie manuell verschieben.

c) Externe Komponenten & Datenübermittlung

Copilot integriert sich tief in das Ökosystem von Microsoft 365 (Graph, OneDrive, SharePoint, Teams) sowie ggf. externe Datenquellen/Agenten. Auch bei guter interner Steuerung bleibt der Punkt: Wann und wie Daten außer- oder über die Tenant-Grenzen hinaus verarbeitet werden.

Beispiel: Web-Suchergebnisse, Drittanbieter-Agenten, die mit Copilot verbunden sind – hier kann externe Verarbeitung stattfinden. Selbst mit sensiblen Daten-Labels kann ein Fehler in einem Connector oder Agenten bedeuten, dass Daten „außer Sicht“ verarbeitet werden.

d) Governance ist ein laufender Prozess – kein Zustand

Kein System ist perfekt. Governance kann die Eintrittswahrscheinlichkeit reduzieren, aber nicht vollständig eliminieren. Wenn ein Agent oder Connector falsch konfiguriert oder ein Drittanbieter-Agent zugelassen wird, kann Datenabfluss entstehen, selbst wenn Policies existieren. Außerdem betrachten viele Organisationen Rollenrechte, Prompt-Policies & Co als „einmal erledigt“.
In Wahrheit:

Rechte ändern sich mit neuen Projekten, Teams, Datenquellen. Wenn neue Datenquellen entstehen muss hier eine konsequente Überprüfung eingerichtet

werden. Wenn Governance-Prozess nicht konsequent betrieben wird, verfällt Sicherheit mit der Zeit, wie typische technische Schulungsergebnisse. Das bedeutet, dass auch bei initial guter Einrichtung langfristig ein Risiko entsteht, wenn nicht fortlaufend gepflegt wird.

Auch wenn Microsoft 365 Copilot aus vielen Perspektiven derzeit die „sicherere" Variante gegenüber freien KI-Browsern darstellt, gilt:

Als Führungspersönlichkeit im technischen Umfeld heißt das:

Copilot ist kein „sicherer Hafen". Es ist **ein Schritt in die richtige Richtung**, aber er erfordert eine sehr strikte Begleitung – und er ersetzt nicht die Notwendigkeit, Datenströme, Rechte und Tools kontinuierlich kritisch zu hinterfragen.

Warum „normale" Browser aktuell noch sicherer sind

Viele Führungskräfte ziehen hier aktuell den falschen Schluss:
„Wenn es *KI-Browser* gibt, dann sind die doch extra dafür gebaut und also sicherer."
Leider ist das Gegenteil der Fall — **zumindest derzeit**.

Der Kernunterschied: Integrationsgrad und Kontrollgrenzen

Ein **KI-Browser** wie Comet oder Arc mit eingebauter KI-Engine ist tief in den Browserkern integriert. Er greift auf Tabs, Verlauf, Cookies, Sessions, gespeicherte Passwörter, Cloud-Zugriffe und deine offenen Dokumente zu, um kontextbezogen zu „helfen".
Das bedeutet:
👉 Er hat Zugriff auf nahezu alles, was du tust, um „intelligent" reagieren zu können.

Wenn dieser Browser kompromittiert wird, dann ist das ganze Nutzungskontinuum betroffen: Inhalte, Logins, gespeicherte Tokens, interne Systeme.

Ein **Standardbrowser** (z. B. Chrome, Edge, Firefox) mit **getrennter KI-Funktion** – z. B. über ein geprüftes Plugin, eine Web-App oder eine interne Plattform – **trennt diese Ebenen technisch**:

- Der Browser bleibt ein Anzeigetool.
- Die KI läuft in einem separaten Prozess oder über eine API mit klarer Authentifizierung und Logging.
- Daten, die an die KI gesendet werden, kannst du filtern, maskieren, kontrollieren und protokollieren.

Diese **Entkopplung** ist der entscheidende Sicherheitsvorteil.

🔐 Wie wirkt sich dieser Sicherheitsvorteil im Detail aus? Hier eine Betrachtung anhand Beispielhafter Angriffswege im Vergleich:

Szenario	KI-Browser (z. B. Comet)	Standardbrowser + KI (z. B. ChatGPT / internes Tool)
1. Prompt Injection (bösartiger Befehl in Webseite)	Hohe Gefahr: KI liest Seite automatisch, kann Anweisung sofort umsetzen (z. B. Daten kopieren, Formulare ausfüllen).	Geringe Gefahr: KI sieht Seite nur, wenn du den Text aktiv kopierst – menschliche Prüfung dazwischen.
2. Credential Theft (Session Hijacking)	Kritisch: KI-Instanz hat Zugriff auf Browser-Sessions, Cookies, Logins.	Kaum Risiko: KI-Tool läuft außerhalb, keine Session-Sharing-Struktur.

Szenario	KI-Browser (z. B. Comet)	Standardbrowser + KI (z. B. ChatGPT / internes Tool)
3. Data Leakage durch Autonomie	Hoch: KI kann automatisierte Aktionen ausführen (z. B. Zahlungen, Uploads).	Minimal: Keine automatischen Aktionen, nur Nutzersteuerung.
4. IT-Governance	Schwach: Neue Tools, proprietäre Logs, kaum einheitliches Auditing.	Stark: Bestehende Sicherheitsrichtlinien, DLP-Systeme, Browser-Policies greifen weiter.

Der zweite große Punkt: Transparenz & Auditfähigkeit

KI-Browser sind derzeit Black Boxes. Du weißt nicht genau,

- wo Daten verarbeitet werden,
- ob sie gespeichert werden,
- ob Logs extern landen,
- oder wie die Modelle trainiert und aktualisiert werden.

In klassischen Browsern mit separater KI-Nutzung hast du:

- **Klare Trennung von Zugriffspfaden** (du entscheidest, wann Daten an die KI gehen),
- **Protokollierbare Schnittstellen** (APIs, Logs, Gateways),
- **Zentral administrierbare Sicherheitspolicies** (SSO, Proxy, DLP).

Mit anderen Worten: Ein Standardbrowser bleibt unter der Kontrolle deiner Unternehmens-IT. Ein KI-Browser führt seine eigenen, schwer einsehbaren Prozesse aus — und macht Sicherheitsmanagement zum Blindflug.

Praktische Faustregel für Führungskräfte

„Alles, was automatisch denkt, aber auf dieselben Daten zugreift, wie du, ohne dass du siehst, wann und wo, ist ein Sicherheitsrisiko."

KI-Browser sind genau das:
Sie kombinieren Kontext (deine Inhalte) mit Autonomie (eigene Entscheidungen). Das ist funktional genial, aber sicherheitstechnisch explosiv. Solange es keine etablierten Enterprise-Standards, API-Isolationsmechanismen und zertifizierte Sandbox-Modelle gibt, gilt:

➡️ **KI ja – aber innerhalb eurer kontrollierten Umgebung.**
➡️ **KI-Browser nein – bis Sicherheitsstandards existieren.**

Was du jetzt konkret tun solltest

Sofort (heute)

- **Verbot für KI-Browser** im Unternehmensnetzwerk.
- **Shadow-Use-Scan:** Wer nutzt Comet, Copilot oder andere Tools bereits?
- **Kurze Policy (1 Seite):** Was darf wohin eingegeben werden – und was nicht?

Kurzfristig (4–8 Wochen)

- **KI-Gatekeeper:** Eine zentrale Plattform, die KI-Zugriffe kontrolliert und filtert.
- **Prompt-Sanitizer:** Maskierung sensibler Daten, bevor sie an externe Systeme gesendet werden.
- **Rollenspezifische Schulungen:** Vertrieb ≠ Entwicklung ≠ Einkauf.

Mittel- bis langfristig

- **Red-Team-Tests:** Simuliere Prompt-Injection und Agenten-Hijacking.
- **Model-Routing:** Interne Modelle für vertrauliche Inhalte, externe nur für offene Recherchen. Deine KI-Plattform sollte diese Wahlmöglichkeiten bieten.
- **Audit & Retention**: Jede KI-Interaktion muss nachvollziehbar und revisionssicher protokolliert werden.

Fazit: Geschwindigkeit ist keine Entschuldigung für Naivität

KI-Browser sind faszinierend – und sie werden bleiben.
Aber im heutigen Reifegrad sind sie für **Unternehmensdaten ein Hochrisikofaktor**.
Wer sie unkontrolliert nutzt, öffnet Hintertüren, die weder IT noch Management überblicken.

Wenn du als Führungskraft Verantwortung trägst, brauchst du **Tempo UND Kontrolle** – nicht das eine auf Kosten des anderen.

Starte jetzt mit einer sicheren KI-Plattform.

Diese bietet dir nicht nur eine hervorragende Performance, sondern die Möglichkeit, klare Spielregeln zu definieren, wer in deinem Unternehmen KI verwendet und wie.

Lass dich nicht von glänzenden Interfaces täuschen – echte Sicherheit entsteht nicht im Frontend, sondern in der Architektur. Mit einer leistungsfähigen Decision Engine kannst du außerdem entscheiden, welche Teilprozesse überhaupt mit KI gelöst werden sollen und welche auf ausgereifte interne Automationstools zurückgreifen.

Auf einer professionellen Plattform laufen diese Prozesse Hand-in-Hand. Ich begleite dich gerne dabei – vom Aufsetzen einer sicheren KI-Plattform, über die Einführung von Trainingsprozessen, bis zur Einführung in deinem Team.

Gemeinsam sorgen wir dafür, dass du KI nutzt, ohne dein Unternehmen zu gefährden.

Anita



Über die Autorin

Anita Renc

KI-Consultant und Business Coach mit über 30 Jahren Industrie- und Führungserfahrung

info@futuresetup.de **futuresetup.de**