



KI-CODE INNOVATION ODER RISIKO?

Innovation mit Weitblick



KI-Speed: Ihr Turbo für 2026, aber mit Sicherheitsgurt!

Künstliche Intelligenz ist der stärkste Hebel, den Schweizer KMU heute haben. Sie ist kein reines IT-Thema mehr, sondern ein strategischer Business-Case: KI spart massiv Zeit, senkt Entwicklungskosten und katapultiert Ihre Innovationsgeschwindigkeit auf ein neues Level.

Doch echter Vorsprung entsteht nur, wenn die Geschwindigkeit nicht auf Kosten der Substanz geht. Während die KI Ihren Code in Rekordzeit schreibt, gilt es, die „versteckten Kosten“ von morgen schon heute zu vermeiden.

DIE LÖSUNG





Die Bittere Wahrheit

KI-Tools wie ChatGPT oder GitHub Copilot steigern die Effizienz massiv, doch sie erzeugen oft eine gefährliche „Sicherheitsscheinwelt“.

Wer die KI ohne klare Richtlinien programmieren lässt, riskiert nicht nur technische Fehler, sondern gefährdet die Existenzgrundlage des Unternehmens durch Sicherheitslücken und rechtliche Fallstricke.

Security



Mühsam, aber Wichtig!

Sicherheit ist kein technisches Feature, sondern eine unternehmerische Notwendigkeit. Die KI wählt oft den „bequemsten“ Weg, nicht den sichersten.

Abfluss von Betriebsgeheimnissen

Die KI schreibt oft interne Passwörter oder Zugangsdaten (API-Keys) direkt in den Quellcode. Sobald dieser Code für Korrekturen erneut in die KI geladen wird, landen Ihre sensiblen Daten auf den Servern der US-Anbieter.

Veraltete Sicherheitsstandards

Da die KI auf Daten der Vergangenheit basiert, schlägt sie häufig Software-Bausteine vor, deren Sicherheitslücken bereits bekannt und für Hacker leicht ausnutzbar sind.

Offene Einfallstore

Um Funktionen schnell zum Laufen zu bringen, deaktiviert die KI oft Schutzwälle (wie CORS-Policies) oder nutzt unsichere Methoden, die Cyber-Angriffe auf Ihre Kundendaten ermöglichen.



Supply Chain

Die „GIFTIGE“ Pille

In der digitalen Welt ist Ihr Code von externen Paketen abhängig. Die KI prüft diese Quellen oft nicht kritisch genug.

Digitale Kuckuckseier

Manchmal „erfindet“ die KI Bibliothekspakete, die gar nicht existieren. Hacker registrieren diese Namen und hinterlegen dort Schadsoftware, die Ihre Mitarbeiter dann unbewusst installieren.

Fremdzugriff über Dritte

Die KI bindet externe Skripte oft ohne digitale Signatur ein. Wird der Server des Anbieters gehackt, wird unbemerkt Schadcode direkt in Ihre Unternehmensanwendung eingeschleust.

DIE LÖSUNG





Die rechtliche Falle für KMU

Als CEO oder CFO tragen Sie die Verantwortung für Urheberrecht und Datenschutz. Die KI kennt das Gesetz nicht.

Die Lizenz-Falle (Copyleft)

Die KI nutzt oft Code-Schnipsel aus Open-Source-Projekten. Wenn dabei versehentlich eine sogenannte GPL-Lizenz verwendet wird, kann dies rechtlich bedeuten, dass Sie Ihre gesamte Eigenentwicklung offenlegen und kostenlos anbieten müssen.

Verstoss gegen die DSGVO

Die KI bindet standardmässig gerne US-Dienste (wie Google Fonts) ein, die Nutzerdaten ohne Einwilligung in die USA übertragen. Dies führt zu direkten Verstössen gegen das Datenschutzgesetz und birgt hohes Bussgeldrisiko.

Das Risiko der “BLACK BOX”



Kurzfristige Einsparungen bei der Entwicklung können langfristig zu massiven Kosten führen.

Abhängigkeit und Wissensverlust

Wenn Ihr Team Code nur noch generiert, statt ihn zu verstehen, verlieren Sie die Kontrolle über die eigene Logik. Bei Problemen kann niemand mehr eingreifen, weil das fundierte Basiswissen fehlt.

Digitales Kartenhaus

Der KI fehlt der strategische Blick für das Ganze. Nach mehreren Änderungen wird der Code so instabil, dass kleine Updates unvorhersehbare Systemausfälle an anderer Stelle verursachen können.



Die Übersicht

Bereich	Risiko	Auswirkung
Datenschutz	DSG-Verstöße	Bussgelder und Reputationsschaden durch US-Datentransfer.
Haftung	Lizenz-Konflikte	Verlust des Schutzes Ihres geistigen Eigentums.
IT-Sicherheit	Hardcoded Secrets	Diebstahl von Firmen- und Kundendaten durch offengelegte Keys.
Stabilität	Black Box Code	Hohe Folgekosten bei Wartung und drohende Systemausfälle.



DIE LÖSUNG

**PASCAL
BORNER**

