

Sicherheit in KI-gestützter Softwareentwicklung

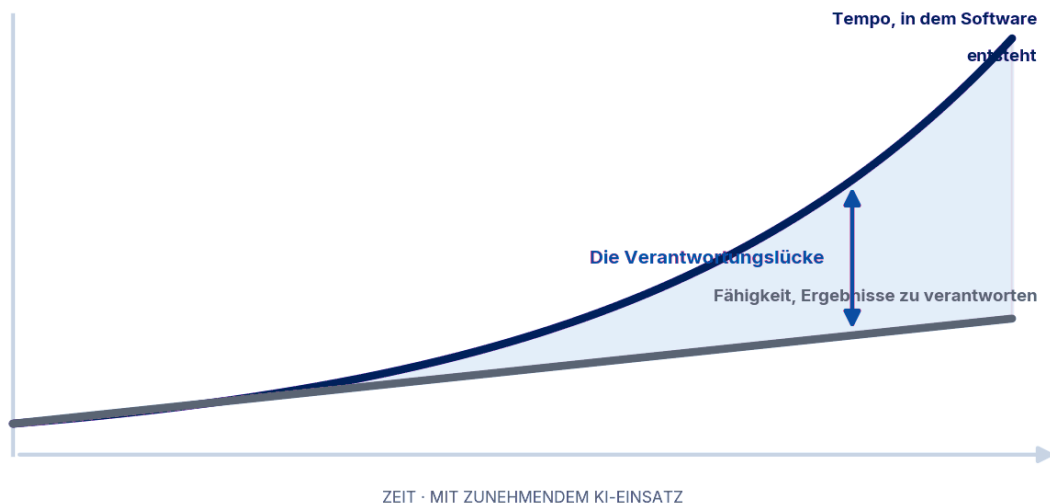
Wie können Unternehmen von Agentic Engineering profitieren?

WORUM ES GEHT

Neue Möglichkeiten kontrolliert nutzen

Seit Herbst 2025 schafft Agentic Engineering neue Realitäten in der Unternehmenswelt. Unter menschlicher Anweisung planen KI-Agenten Entwicklungsaufgaben und setzen diese selbstständig um. Durch diese enormen Fortschritte verändert sich Softwareentwicklung grundlegend. Aufgaben, die vor Kurzem einen Personenmonat gebunden haben, können heute in Tagen gelöst werden. Mit diesem Zuwachs an Geschwindigkeit ist der Einsatz von KI in der Softwareentwicklung auch im Mittelstand angekommen.

Was ist das Risiko dieser Entwicklung? Die menschliche Fähigkeit, ein KI-generiertes Ergebnis fachlich zu beurteilen, ist begrenzt. Sie bleibt an qualifizierte Personen gebunden, die mit der bestehenden Software im Haus vertraut sind. Zwischen dem, was ein Unternehmen an Code herstellen kann, und dem, was es prüfen und damit verantworten kann, öffnet sich eine Lücke.



Diese Lücke ist ein Engpass beim Einsatz von Agentic Engineering. Sie begrenzt die neuen Möglichkeiten, Software neu zu entwickeln oder bestehende Systeme zu überarbeiten. Wird sie geschlossen, lässt sich Verantwortung schrittweise an Agenten übergeben, und der Zuwachs kommt im Ergebnis an.

KI in der Softwareentwicklung muss sicher und beherrschbar sein.

Wo Software in Unternehmen entsteht

Softwareentwicklung in Unternehmen konzentriert sich im Wesentlichen auf drei Bereiche.

Der erste ist die **laufende Anpassung** vorhandener Anwendungen. Hier werden Fehler behoben, neue fachliche Anforderungen umgesetzt, gesetzliche Vorgaben nachgezogen und Schnittstellen zu Kunden, Lieferanten und Partnern gepflegt. Dieser Bereich bindet oft den größten Teil der Entwicklungskapazität.

Der zweite ist die **Modernisierung**. Anwendungen, die seit vielen Jahren im Einsatz sind, werden auf eine neue technische Grundlage gehoben, entflochten oder abgelöst. Solche Vorhaben unterblieben bislang häufig, weil ihr Aufwand in keinem Verhältnis zum erkennbaren Nutzen stand.

Der dritte ist die **Neuentwicklung**. Fachbereiche benötigen Anwendungen, die es als Standardsoftware nicht gibt. Auch hier gab bislang der Aufwand den Ausschlag.

In allen drei Bereichen können KI-Agenten heute einen wachsenden Teil der Arbeit übernehmen. Damit rückt eine Frage in den Vordergrund: Wie stellen Unternehmen sicher, dass eine Änderung genau das bewirkt, was beabsichtigt war? Ohne Vorkehrungen gelangt Software in den Betrieb, deren Verhalten niemand vollständig geprüft hat. Die Folgen treffen das Geschäft. Ein Preis wird falsch berechnet, eine Schnittstelle zum Kunden bricht ab, ein Auftrag bleibt liegen, ein Datenzugriff bleibt offen.

Eine naheliegende Lösung wäre, die menschliche Prüfung entsprechend auszuweiten. Dieser Weg trägt nicht weit. Eine Änderung fachlich zu beurteilen setzt voraus, dass die Zusammenhänge und das bestehende System bekannt sind. Dieses Kenntnis ist an erfahrene Personen gebunden. Sie lässt sich weder kurzfristig einkaufen noch in dem Tempo aufbauen, in dem KI-Agenten Ergebnisse liefern. Wer die gewonnene Geschwindigkeit nutzen will, muss die Prüfkapazität auf anderem Wege ausbauen.

DIE ANTWORT

Die Prüfstraße als Fundament

Da die menschliche Prüfung nicht mitwachsen kann, muss die Prüfung selbst automatisiert werden. Das leistet eine Prüfstraße.

Eine Prüfstraße ist eine Kette automatischer Prüfungen. Jede Änderung durchläuft sie, bevor sie in den Betrieb gelangt. Technisch stützt sie sich auf die Werkzeuge, die in der Entwicklung als CI/CD-Pipeline bekannt sind. Sie geht darüber hinaus, weil sie neben dem Bau der Software auch den Nachweis über deren fachliches Verhalten führt.

Vier Prüfungen laufen dabei ab. Die erste kontrolliert die Form. Entspricht der Code den Unternehmensstandards? Die zweite sucht nach Sicherheitslücken im eigenen Code, etwa nach Zugangsdaten, die versehentlich im Quelltext stehen. Die dritte prüft fremde Bausteine, also Software aus anderer Quelle, die im eigenen Produkt mitläuft. Für sie werden laufend Schwachstellen gemeldet, oft lange nach dem Einbau. Die vierte beurteilt das fachliche Verhalten. Im Bestand weist sie nach, dass sich nichts unbeabsichtigt verschoben hat. Bei einer Neuentwicklung weist sie nach, dass das Ergebnis der fachlichen Vorgabe entspricht.

Alle vier Prüfungen sind notwendig. Die vierte verlangt die meiste Vorbereitung, weil sie eine Sammlung automatischer Tests voraussetzt. Jeder einzelne Test prüft einen fachlichen Fall, etwa eine Preisberechnung unter bestimmten Bedingungen. Die Tests laufen unabhängig voneinander und in kurzer Zeit. Zusammen bilden sie ein Netz, das die wichtigsten Abläufe abdeckt. Je dichter das Netz, desto weniger kann unbemerkt hindurchfallen.

An dieser Stelle greift der KI-Agent in die Prüfstraße ein. Er erzeugt eine Änderung und schickt sie durch die Kette. Fällt eine Prüfung negativ aus, erhält er die Rückmeldung und bessert nach. Das wiederholt er, bis alle Prüfungen bestanden sind. Erst dann legt er das Ergebnis einem Menschen vor. Ohne das Netz fehlt ihm diese Rückmeldung, und die Beurteilung fällt vollständig auf den Menschen zurück.

Für das Unternehmen ändert sich damit die Rolle des Menschen in der Entwicklung. Er gibt Ziele und fachliche Kriterien vor. Die Kontrolle jedes einzelnen Ergebnisses entfällt. Freigeben muss er weiterhin, denn wer Software verantwortet, kann diese Verantwortung nicht abgeben. Die Freigabe wird jedoch zur Bestätigung, weil die technische Prüfung bereits gelaufen ist.

Aufbauen, dann ausbauen

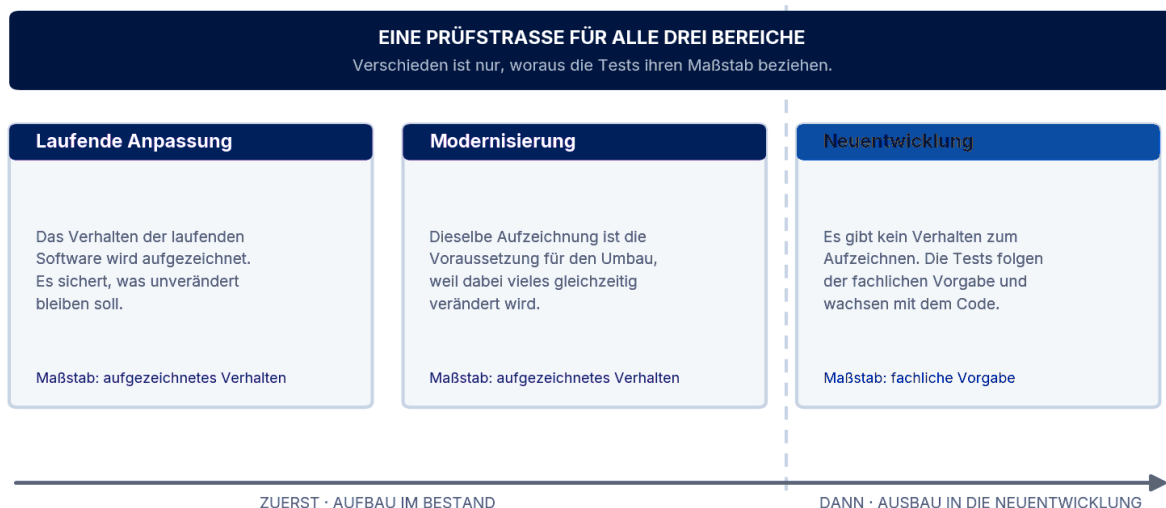
Alle drei Bereiche aus dem vorigen Abschnitt brauchen eine Prüfstraße: die laufende Anpassung, die Modernisierung und die Neuentwicklung.

Bewährt hat sich, die Prüfstraße zunächst im Softwarebestand aufzubauen und sie danach in der Neuentwicklung einzusetzen. Im Bestand ist das erwartete Verhalten bereits festgelegt, jeder Test lässt sich also unmittelbar gegen die laufende Software prüfen. Darüber hinaus kann Erfahrung in einem bekannten Bereich aufgebaut werden. Das senkt die Einstiegshürden und fördert die Akzeptanz.

Die Prüfstraße wird also einmal aufgebaut und danach sukzessive ausgerollt. Jeder Test braucht jedoch einen Maßstab, also die Angabe, was als richtiges Verhalten gilt. Dieser Maßstab hat je Bereich eine andere Basis.

Im Bestand liefert die laufende Software den Maßstab selbst. Ihr Verhalten wird aufgezeichnet und festgehalten, bevor jemand eingreift. Bei einer Anpassung sichert das die Stellen, die unverändert bleiben sollen. Bei einer Modernisierung ist es die Voraussetzung für den Umbau, weil dabei vieles gleichzeitig verändert wird.

Bei einer Neuentwicklung gibt es noch kein Verhalten, das sich aufzeichnen ließe. Der Maßstab kommt deshalb aus der fachlichen Vorgabe, und die Tests entstehen zusammen mit dem Code.



Die Prüfstraße ist keine Maßnahme neben den drei Bereichen. Sie ist ihre gemeinsame Voraussetzung.

AUS UNSERER ERFAHRUNG

Was über den Erfolg entscheidet

Der Aufbau einer Prüfstraße ist technisch überschaubar. Woran Projekte scheitern, hat andere Gründe. Vier davon sehen wir immer wieder. Alle vier lassen sich vermeiden, wenn sie zu Projektbeginn benannt und geregelt werden.

Wo Projekte ins Stocken geraten

Fehlende Verbindlichkeit. Der Aufbau läuft neben dem Tagesgeschäft. Ohne fest zugewiesene Personen und Zeiten verliert er gegen jede Tagespriorität und bleibt nach wenigen Wochen liegen.

Kritischer Kern nicht bestimmt. Fehler gelangen über Änderungen in die Software. Wo zuerst abgesichert wird, richtet sich deshalb nach zwei Größen: dem möglichen Schaden und der Häufigkeit der Änderungen. Ohne diese Bewertung verteilt sich der Aufwand über den gesamten Bestand. Die Absicherung wird an keiner Stelle belastbar.

Prüfungen ohne Konsequenz. Werden die Prüfungen als Hinweis eingerichtet und nicht als Bedingung für die Freigabe, sammeln sich unbeachtete Befunde. Das Unternehmen hält sich für abgesichert, ohne es zu sein.

Netz ohne Kalibrierung. Agenten erzeugen in kurzer Zeit sehr viele Tests. Ohne Steuerung prüfen viele davon Nebensächliches, und die Laufzeit der Prüfstraße steigt. Es bleibt unklar, welche Risiken tatsächlich abgedeckt sind.

Was erfolgreiche Projekte anders machen. Sie behandeln den Aufbau als Projekt, mit eigener Leitung, festen Zwischenzielen und benannten Verantwortlichen. Sie sichern zuerst die Bereiche ab, in denen ein Fehler am meisten kostet und am häufigsten entstehen kann, und weiten den Umfang erst danach aus.

Sie messen von Beginn an. Erhoben wird, wie lange es heute dauert, bis ein Fehler nach der Auslieferung auffällt. Aus den Vorfällen der zurückliegenden Monate ergibt sich ein Mittelwert, häufig mehrere Wochen. Diese Zahl ist die Führungskennzahl des Projekts. Sie sinkt mit jedem abgesicherten Bereich, und daran lässt sich der Fortschritt ablesen.

Sie führen die Veränderung. Die Entwickler geben Kontrollschritte ab, die sie bisher von Hand ausgeführt haben, und geben dafür fachliche Kriterien vor. Die IT-Leitung entscheidet über Schwellenwerte und Freigaberegeln, der Fachbereich liefert die fachlichen Vorgaben.

DER NUTZEN

Ihre Potenziale

Jedes Projekt braucht einen Grund. Für den Aufbau einer Prüfstraße sind es vier.

Fehler werden früh sichtbar. Heute vergehen zwischen einer fehlerhaften Auslieferung und ihrer Entdeckung oft Wochen. Mit einer Prüfstraße sind es Minuten. Aus einem Vorfall, der Kunden erreicht und Nacharbeit auslöst, wird eine kurze Korrektur.

Prüfkapazität wird frei. Erfahrene Entwickler prüfen heute jede Änderung von Hand. Nach dem Aufbau übernimmt die Prüfstraße den größten Teil davon. Die gewonnene Zeit fließt in Arbeit, die sich nicht automatisieren lässt: Anforderungen klären, Architektur entscheiden, Kriterien festlegen.

Vorhaben werden wirtschaftlich, die es bisher nicht waren. Modernisierungen und Neuentwicklungen scheiterten bislang häufig am Aufwand. Mit KI-Agenten sinkt dieser Aufwand deutlich, mit einer Prüfstraße wird das Ergebnis verantwortbar. Erst beides zusammen macht solche Vorhaben attraktiv.

Agentic Engineering wird skalierbar. Ohne belastbare Prüfung bleibt der Einsatz von Agenten auf unkritische Randbereiche beschränkt. Mit ihr lässt sich der Anteil schrittweise ausweiten. Der Zuwachs an Geschwindigkeit kommt damit im Ergebnis an.



Die Prüfstraße entscheidet darüber, wie viel Verantwortung ein Unternehmen an KI übergeben kann. Sie ist die Voraussetzung dafür, dass sich Geschwindigkeit auszahlt.

IHR NÄCHSTER SCHRITT

Verorten Sie sich

Vier Fragen zeigen, wo Ihr Unternehmen heute steht.

Prüfen Sie Ihre Ausgangslage

- 01** Wie lange dauert es, bis wir wissen, dass eine Änderung etwas beschädigt hat?
- 02** Wenn jemand einen Test entfernt, bemerkt das jemand?
- 03** Schreibt dieselbe Instanz die Prüfung, die auch das Ergebnis liefert?
- 04** Wer entscheidet, welcher fremde oder KI-erzeugte Code ins Produkt darf?

Ihre Antworten sind der Ausgangspunkt. In einem Deep-Dive-Workshop ordnen wir sie ein, bestimmen Ihren Ausgangswert und legen die ersten Schritte fest. Der Aufbau verläuft danach in Phasen, von denen jede für sich einen Wert liefert. Sie entscheiden nach jedem Schritt neu, wie es weitergeht.

Kühl & Barz begleitet mittelständische Unternehmen beim sicheren Einsatz von KI in der Softwareentwicklung. Sprechen Sie uns an.