WEBMCP VERSTÄNDLICH ERKLÄRT: WAS ES IST UND WAS NICHT

Veröffentlicht am 23. Oktober 2026 von Maya

Wie kann ein KI-Assistent auf Deiner Website **eine Aufgabe erledigen**? Produktinformationen lesen ist das eine. Die richtige Variante auswählen, einen Warenkorb zusammenstellen oder eine Buchung vorbereiten verlangt zusätzliche Funktionen. WebMCP soll Websites dafür **einen definierten Zugang geben**, statt Agenten allein durch die sichtbare Oberfläche navigieren zu lassen.

Das ist bereits keine Theorie mehr: Shopify stellt WebMCP-Tools auf jeder Liquid-Storefront bereit. OpenAI unterstützt entsprechende Websitefunktionen im integrierten Browser der ChatGPT-Desktop-App, und Cloudflare bietet eine Entwickler-Vorschau für die Einbindung an. Hinter dem Kürzel steckt allerdings etwas anderes als eine weitere Möglichkeit, mit KI Texte zu erstellen oder bei Google besser gefunden zu werden.

WAS IST WEBMCP?

WebMCP steht für Web Model Context Protocol. Gemeint ist ein **vorgeschlagener Webstandard**, mit dem Websites bestimmte Funktionen **als Werkzeuge für KI-Agenten bereitstellen können**. Ein Agent ist dabei ein KI-Assistent, der mithilfe solcher Werkzeuge Aufgaben ausführt, anstatt lediglich eine Antwort zu formulieren.

Ein solches Werkzeug könnte beispielsweise Produkte suchen, einen Bestellstatus abfragen oder eine Auswahl in einem Formular übernehmen. Die Website beschreibt, was die Funktion macht und welche Eingaben sie benötigt. Der Agent kann sie daraufhin gezielt aufrufen. Technisch lassen sich solche Werkzeuge unter anderem mit JavaScript registrieren; sie erhalten einen Namen, eine Beschreibung und ein festgelegtes Schema für ihre Eingaben.

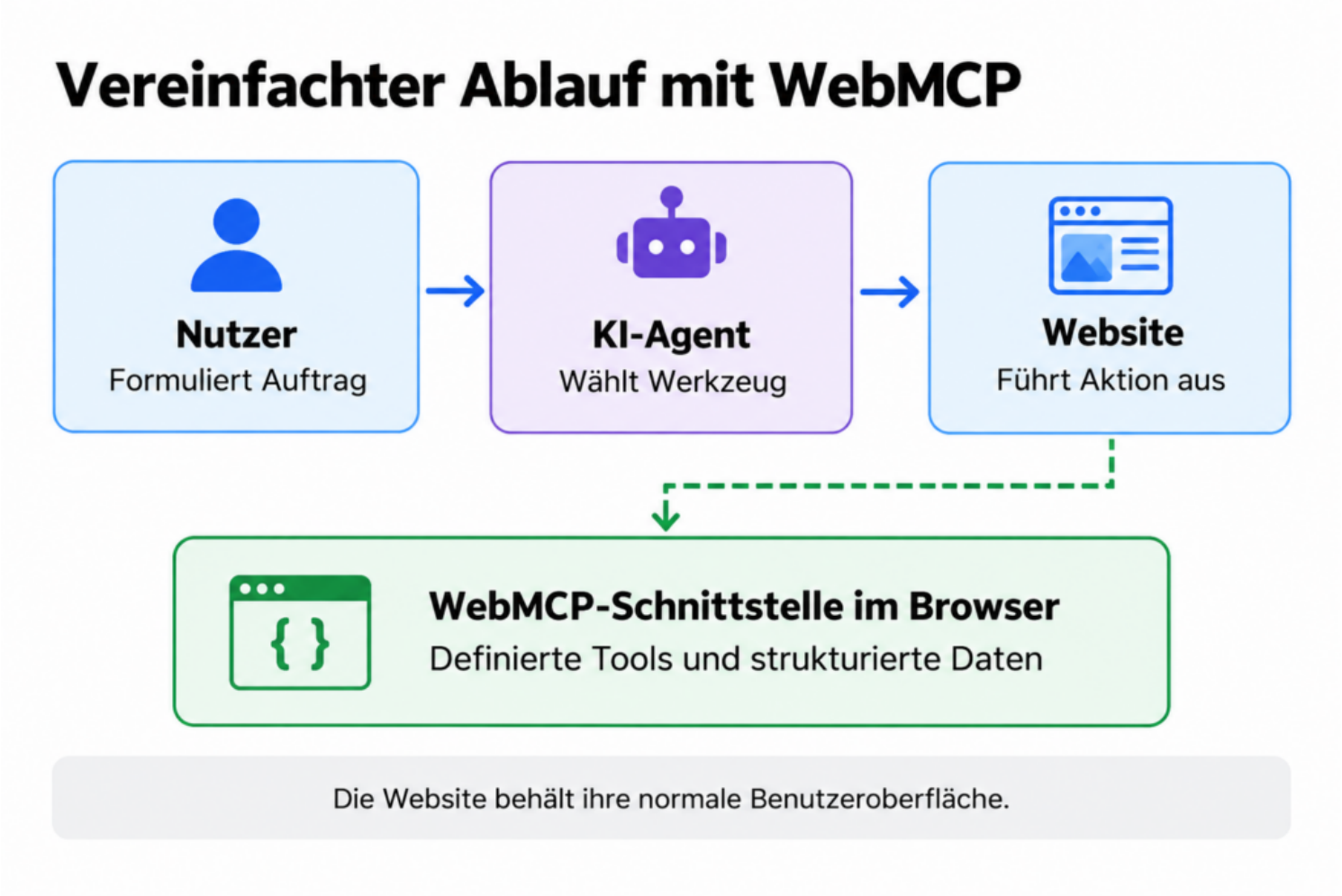
Wichtig ist der Entwicklungsstand: WebMCP ist noch kein verabschiedeter W3C-Webstandard. Die Spezifikation wird von der Web Machine Learning Community Group veröffentlicht und **ausdrücklich als Entwurf geführt**. Bereits verfügbare Produkte und ein noch nicht abgeschlossener Standardisierungsprozess schließen sich hier also nicht aus.

WIE FUNKTIONIERT WEBMCP AUF EINER WEBSITE?

Nehmen wir einen Onlineshop für Büromöbel. **Ein Kunde bittet seinen KI-Assistenten**: „Suche einen schwarzen Bürostuhl unter 300 Euro und lege ein verfügbares Modell in den Warenkorb." Für einen Menschen wäre das eine überschaubare Aufgabe: Suchbegriff eingeben, Ergebnisse filtern, Produkt auswählen und auf den Warenkorb-Button klicken.

Ein Browser-Agent muss ohne passende Schnittstelle zunächst erkennen, wie die Seite funktioniert. Er kann beispielsweise den Seitenaufbau auswerten und Klicks oder Texteingaben nachahmen. Dabei können ungewöhnliche Bedienelemente, zusätzliche Dialoge oder Änderungen am Layout den Ablauf erschweren. WebMCP ergänzt diesen Weg um direkt aufrufbare Websitefunktionen.

Im Beispiel könnte der Agent Werkzeuge für die Katalogsuche, die Produktabfrage und die Warenkorbverwaltung verwenden. Shopify bietet dafür etwa search_catalog, get_product und update_cart an. Der Agent entscheidet anhand des Auftrags und der Werkzeugbeschreibungen, welche Funktion er benötigt. Die Aktionen finden in der laufenden Sitzung des Kunden statt; Änderungen am Warenkorb betreffen den Warenkorb, den der Kunde tatsächlich sieht.



Die normale Benutzeroberfläche bleibt erhalten. Der Kunde kann weiterhin selbst durch den Shop navigieren und das Ergebnis prüfen. WebMCP ergänzt die Website um einen Zugang für den Agenten, während Mensch und Assistent mit derselben geöffneten Seite arbeiten. Das ist besonders dann hilfreich, wenn eine Aufgabe gemeinsam bearbeitet und zwischendurch kontrolliert werden soll.

WAS SHOPIFY, OPENAI UND CLOUDFLARE BEREITS ANBIETEN

Die drei Anbieter übernehmen unterschiedliche Aufgaben. Shopify stellt Funktionen auf Shop-Websites bereit, OpenAI liefert eine Umgebung, in der ein Assistent solche Funktionen nutzen kann, und Cloudflare vereinfacht die technische Bereitstellung. Diese Unterschiede sind wichtig, wenn Du beurteilen möchtest, was für Deine eigene Website bereits möglich ist.

SHOPIFY: WERKZEUGE AUF JEDER LIQUID-STOREFRONT

Shopify hat im August 2026 angekündigt, WebMCP-Tools auf jeder Liquid-Storefront bereitzustellen, also auf allen mit Shopifys Liquid-Templates aufgebauten Shop-Oberflächen. Händler müssen dafür nichts installieren oder konfigurieren. Die Werkzeuge decken Katalogsuche, Variantenauswahl, Warenkorbänderungen und die Navigation zum Checkout ab. Nutzbar sind sie nur mit einem kompatiblen Agenten in einer unterstützten Browserumgebung.

Wichtig ist die Grenze zwischen Warenkorb und Bestellung: Das Storefront-Werkzeug führt nur zur Kasse. Für unterstützte Checkouts dokumentiert Shopify eigene Werkzeuge, die den Checkout lesen, aktualisieren und eine Bestellung nach Bestätigung durch den Käufer abschließen. Eine vorbereitete Produktauswahl ist also keine automatisch ausgelöste Bestellung.

OPENAI: CHATGPT KANN WEBSITE-TOOLS VERWENDEN

OpenAI nennt seine WebMCP-Umsetzung „Site tools“, auf Deutsch Website-Tools. Im integrierten Browser der ChatGPT-Desktop-App erkennt und verwendet ChatGPT passende Werkzeuge einer geöffneten Website. Was verfügbar ist, hängt unter anderem von Konto, Modell und Seite ab. „ChatGPT unterstützt WebMCP“ heißt also nicht, dass jeder Nutzer jede Website so bedienen kann.

Zudem unterstützt OpenAI nicht alle Einbindungsarten: Werkzeuge in eingebetteten Seiten, sogenannten iframes, erkennt ChatGPT nicht. Ein extern eingebundenes Buchungsformular ist daher nicht automatisch nutzbar. Die Umsetzung muss zur vorgesehenen Browser- und Agentenumgebung passen.

CLOUDFLARE: DIE EINBINDUNG KANN VOR DEM EIGENTLICHEN WEBSERVER ERFOLGEN

Cloudflares Entwickler-Vorschau ergänzt ausgelieferte Webseiten um ein kleines Skript, das ausgewählte Werkzeugpakete registriert. Der Websitecode auf dem Webserver bleibt dabei unverändert. Zu den ersten Paketen gehören die Anbindung vorhandener MCP-Server und das Auslesen von Herkunftsinformationen bei Bildern.

Die Einbindung wird so einfacher, eine vollständige Agenten-Anbindung für beliebige Geschäftsprozesse entsteht dadurch aber nicht: Hat Deine Website keine nutzbare Terminbuchung, schafft das Skript sie auch nicht. Was ein Agent erledigen kann, hängt weiterhin von den

bereitgestellten Werkzeugen ab.

WAS WEBMCP NICHT IST

Die ähnlichen Begriffe rund um KI-Suche, Schnittstellen und Automatisierung machen die Einordnung unnötig schwierig. Für Deine Website lohnt es sich deshalb, drei Fragen auseinanderzuhalten: Wie wird sie gefunden? Wie werden Informationen zugänglich? Und wie lassen sich ihre Funktionen bedienen? **WebMCP** beschäftigt sich vor allem mit der Interaktion auf einer besuchten Website.

KEIN ERSATZ FÜR SEO ODER GEO

WebMCP entscheidet nicht darüber, warum ein Unternehmen in einer Suchantwort genannt wird. Die Werkzeuge werden für einen kompatiblen Agenten zugänglich, wenn er die betreffende Website besucht. Aus dieser technischen Bedienbarkeit lässt sich deshalb **kein automatischer Vorteil bei Rankings oder KI-Empfehlungen ableiten**. Eine Website kann gut bedienbare Funktionen anbieten und trotzdem kaum gefunden werden.

Für Googles KI-Suchergebnisse gelten laut Google weiterhin die grundlegenden SEO-Empfehlungen. Um in AI Overviews oder im AI Mode berücksichtigt zu werden, sind keine zusätzlichen speziellen Optimierungen erforderlich - lediglich der Fokus auf E-E-A-T ist wichtig. WebMCP ersetzt somit weder hilfreiche Inhalte noch die technische Zugänglichkeit einer Website für die Suche.

Die Bereiche können sich überschneiden: Auch eine Datenschnittstelle kann Aktionen ermöglichen, und WebMCP kann Informationen abrufen, ohne etwas zu verändern. Für die Planung hilft die Unterscheidung trotzdem, weil eine bessere Auffindbarkeit und eine zuverlässigere Bedienung unterschiedliche Ziele sind.

NICHT DASSELBE WIE EIN MCP-SERVER

Das Model Context Protocol, kurz MCP, **verbindet KI-Anwendungen mit externen Systemen**. Darüber können beispielsweise Informationen aus Datenbanken abgerufen oder Aufgaben in anderen Anwendungen ausgeführt werden. **MCP ist also nicht auf das Lesen von Daten beschränkt**. WebMCP konzentriert sich dagegen auf Funktionen, die eine Website im Browser bereitstellt.

Frage	MCP	WebMCP
Wo werden die Funktionen bereitgestellt?	Über einen lokalen oder entfernten MCP-Server.	Über die geöffnete Webseite im Browser.
Muss dafür eine Website geöffnet sein?	Nicht grundsätzlich.	Ja. Die Werkzeuge sind an den jeweiligen Seitenkontext gebunden.

Was kann damit passieren?	Informationen abrufen und Aktionen in angebundenen Systemen ausführen.	Informationen abrufen und Aktionen auf der Website ausführen, in der laufenden Sitzung des Nutzers.
Wofür eignet sich der Ansatz?	Für Verbindungen zu Diensten und Unternehmenssystemen.	Für die Zusammenarbeit von Nutzer und Agent auf einer Website.

Beide Ansätze können sich ergänzen. Ein Unternehmen muss sich deshalb nicht grundsätzlich für einen von beiden entscheiden; ausschlaggebend ist, wo die gewünschte Funktion gebraucht wird. Google beschreibt WebMCP ausdrücklich weder als Ersatz noch als bloße Erweiterung von MCP.

Dein Unternehmenswissen auch ohne Websitebesuch für KI-Assistenten nutzbar machen?
Mit stellen wir freigegebene Informationen und definierte Funktionen über eine gemanagte KI-Unternehmensschnittstelle für kompatible KI-Assistenten bereit.

KEIN CHATBOT, DEN DU AUF DEINER WEBSITE EINBAUST

Durch WebMCP erscheint nicht automatisch ein Chatfenster auf Deiner Website. Der Ansatz ermöglicht vielmehr, dass ein unterstützter Assistent auf bereitgestellte Websitefunktionen zugreift. Auch eine mit KI erstellte Website besitzt deshalb nicht automatisch WebMCP-Werkzeuge: Die Art der Websiteerstellung und die spätere Bedienbarkeit durch einen Agenten sind zwei verschiedene Dinge.

FÜR WELCHE UNTERNEHMEN KÖNNTE WEBMCP INTERESSANT WERDEN?

Aus unserer Sicht lohnt sich ein genauerer Blick vor allem dort, wo Besucher auf einer Website mehrere zusammenhängende Schritte erledigen müssen. Denkbare Einsatzfelder sind **umfangreiche Produktkataloge, Konfiguratoren, Terminbuchungen und Kundenportale**. Der mögliche Nutzen liegt dann darin, eine konkrete Aufgabe zu erleichtern, nicht darin, möglichst viele Funktionen mit einem KI-Etikett zu versehen.

Bei einem technischen Händler könnte ein Agent beispielsweise Komponenten anhand vorgegebener Eigenschaften vergleichen und eine Angebotsanfrage vorbereiten. Ein Dienstleister

könnte freie Termine für eine bestimmte Leistung abfragbar machen. In einem Kundenportal wäre denkbar, eine vorhandene Bestellung aufzurufen und daraus eine erneute Anfrage zusammenzustellen. Das sind mögliche Anwendungen; sie setzen jeweils passende Funktionen und die erforderlichen Zugriffsrechte voraus.

Für eine kleine Unternehmenswebsite, deren wichtigste Aufgabe die Darstellung von Leistungen und Kontaktdaten ist, setzen wir die Prioritäten anders. Wenn Interessenten das Angebot noch nicht verstehen oder der Kontaktweg unklar ist, sollte zunächst daran gearbeitet werden.

WO DIE GRENZEN UND RISIKEN LIEGEN

DIE UNTERSTÜTZUNG IST NOCH NICHT ÜBERALL VORHANDEN

Im offiziellen Implementierungsverzeichnis werden unter anderem ChatGPT Desktop, Testprogramme für Chrome und Edge sowie experimentelle Unterstützung in Brave aufgeführt. Eine allgemeine Verfügbarkeit über alle gängigen Browser hinweg ist damit nicht gegeben. Für ein Websiteprojekt reicht es deshalb nicht, die Werkzeuge erfolgreich zu registrieren: Sie müssen mit den Agenten und Browsern getestet werden, die später tatsächlich eingesetzt werden sollen.

EINE VERSTÄNDLICHE WERKZEUGBESCHREIBUNG IST NOCH KEINE ABSICHERUNG

Ein Werkzeug sollte eindeutig erkennen lassen, ob es nur Informationen abruft, einen Vorgang vorbereitet oder eine verbindliche Aktion ausführt. „Termin anzeigen“ und „Termin buchen“ dürfen nicht versehentlich dasselbe bedeuten. Google empfiehlt klare Funktionsbeschreibungen, verlässliche Eingabeprüfungen und nachvollziehbare Fehlermeldungen. Eine wohlformulierte Beschreibung ersetzt die Prüfung im Programmcode nicht.

Dazu kommt **das Risiko manipulierter Inhalte**. Bei sogenannter Prompt Injection können Anweisungen in Websiteinhalten oder Werkzeugantworten versuchen, den Agenten von seinem eigentlichen Auftrag abzubringen. Google weist ausdrücklich auf dieses Problem hin. Für folgenreiche Aktionen sollten Entwickler zusätzliche Schutzmechanismen und Bestätigungen vorsehen, statt sich allein auf das Verhalten des Modells zu verlassen.

OpenAI prüft Website-Tool-Aufrufe zusätzlich und beschreibt Kontrollen gegen unautorisierte Datenweitergabe und Aktionen außerhalb des Nutzerauftrags. Solche Prüfungen reduzieren Risiken, machen aber nicht jede Website oder Werkzeugantwort vertrauenswürdig. Gerade bei Käufen, Änderungen an Kundendaten oder anderen sensiblen Vorgängen bleibt eine kontrollierbare Umsetzung erforderlich.

WAS HEISST DAS FÜR DEINE WEBSITE?

WebMCP ist in echten Produkten angekommen, aber noch nicht überall nutzbar, und jede Funktion braucht klare Grenzen. Ob sich der Aufwand lohnt, entscheidet deshalb weniger die Technik als die Frage, **wo KI-Assistenten Deinen Kunden heute nicht zuverlässig weiterhelfen können.** Typische Hinweise darauf sind:

- Kunden bleiben bei einem Ablauf auf Deiner Website regelmäßig hängen, etwa bei der Produktsuche, einer Konfiguration oder der Terminvereinbarung.
- Dieselben beratungsintensiven Fragen landen immer wieder bei Deinem Team, zum Beispiel zu Einsatzbereichen, Kompatibilitäten oder der passenden Variante.
- Wichtiges Fachwissen steht gar nicht auf der Website, sondern steckt in Datenblättern, Preislisten oder der Erfahrung Deiner Mitarbeiter.
- Informationen ändern sich häufig, etwa Verfügbarkeiten, Lieferzeiten oder freie Termine, und ein KI-Assistent kann sie ohne aktuelle Quelle nur schätzen.
- Auf die Beratung folgt ein klarer nächster Schritt, etwa eine Anfrage oder ein Angebot, den ein Assistent vorbereiten könnte.

Nur der erste Punkt betrifft unmittelbar die Bedienung Deiner Website. Für die übrigen kann auch ein Zugang sinnvoll sein, über den verbundene KI-Assistenten freigegebene Informationen abrufen und Anfragen vorbereiten, ohne dass Deine Website dafür geöffnet sein muss. Das ist die zweite Ebene aus der Grafik oben. Trifft keiner der Punkte zu, bringen bessere Inhalte oder eine klarere Benutzerführung meist mehr.

FAZIT: WEBMCP BETRIFFT DIE NUTZUNG DEINER WEBSITE, NICHT AUTOMATISCH IHRE SICHTBARKEIT

WebMCP gibt KI-Agenten einen definierten Zugang zu Websitefunktionen. Die bisherigen Umsetzungen zeigen, dass dieser Ansatz bereits praktisch nutzbar ist, während Standard und Unterstützung weiterentwickelt werden. Für Unternehmen mit komplexen digitalen Abläufen kann sich deshalb ein Test lohnen. Eine allgemeine Pflicht zur Einführung lässt sich daraus nicht ableiten. Web Machine Learning

Für Deine Planung beginnt alles bei der Aufgabe Deines Kunden: Was soll auf Deiner Website leichter funktionieren, und wo entstehen heute Schwierigkeiten? Ist das geklärt, lässt sich beurteilen, ob bessere Inhalte, eine überarbeitete Benutzerführung, eine Datenschnittstelle oder WebMCP die passende Maßnahme ist.

Du möchtest Deine Website weiterentwickeln und klären, welche Rolle KI-Agenten dabei spielen sollten? Sprich mit uns über Deine Website und die Abläufe dahinter. Gemeinsam prüfen wir, **welche Verbesserungen Deinen Kunden konkret helfen** und welche technischen Ergänzungen dafür sinnvoll sind.