expertenReport

Quelle: mip Consult GmbH

Low-Code, KI und Schatten-IT: Wie Unternehmen die Kontrolle behalten

Low-Code-Plattformen und KI-gestützte Tools ermöglichen es Fachabteilungen, schnell eigene Anwendungen zu entwickeln. Gleichzeitig wächst damit das Risiko neuer Formen von Schatten-IT. Dr. Johann Sell von der mip Consult GmbH erläutert im Gastbeitrag, warum Transparenz, klare Governance-Strukturen und eine enge Zusammenarbeit zwischen IT und Fachbereichen entscheidend sind, um Innovation und Sicherheit miteinander zu verbinden.

Existiert etwa eine Vielzahl selbstentwickelter Tools, von denen die zentrale IT keine Kenntnis hat, kommt es zu Problemen. Niemand weiß dann genau, welche Daten verarbeitet werden, ob sie verschlüsselt sind, wo sie gespeichert werden oder wer Zugriff darauf hat. Besonders kritisch würde es, wenn personenbezogene Daten, vertrauliche Kundeninformationen oder Geschäftsgeheimnisse in solchen Anwendungen landeten. Ohne technische Schutzmaßnahmen, Dokumentation und klare Verantwortlichkeiten entstünden so massive Angriffsflächen, sowohl für Cyberangriffe als auch für regulatorische Verstöße.

Verzahnung elementar

Hinzu kommt die Gefahr von Abhängigkeiten: Werden beispielsweise Low-Code-Lösungen von einzelnen Mitarbeitenden erstellt, ohne saubere Übergabe oder Wartungskonzept, treten schnell Probleme auf. Verlässt diese Person dann das Unternehmen, bleibt eine geschäftskritische Anwendung zurück, die niemand versteht. Technische Schulden, Sicherheitslücken und Betriebsrisiken sind die Folge. Zudem tritt das Risiko auf, dass Integrationen mit anderer bestehender Unternehmenssoftware – etwa einer zentralen Consent-and-Preference-Management-Platform (CPMP) – nicht mitgedacht oder aufgrund der Komplexität bewusst missachtet wird. Gerade beispielsweise CPMP müssen stark integriert sein, um die geforderte Einwilligungsdokumentation korrekt durchzuführen. Verbote sind jedoch keine Lösung. Wer Low-Code-Plattformen pauschal untersagt, fördert Schatten-IT nur weiter, denn die fachlichen Anforderungen bleiben bestehen. Stattdessen braucht es einen strukturierten Ansatz: Unternehmen müssen klare Rahmenbedingungen schaffen, die Innovation ermöglichen und gleichzeitig Sicherheit gewährleisten. Dazu gehören verbindliche Governance-Modelle, definierte Freigabeprozesse, Sicherheitsstandards und dokumentierte Entwicklungsrichtlinien für Fachabteilungen sowie ein technisches Framework, welches zentral bereitgestellt wird und Integration ermöglicht und vereinfacht.

Ein wichtiger Erfolgsfaktor ist die enge Zusammenarbeit zwischen IT, Datenschutz und Fachbereichen. Die IT sollte nicht als Gatekeeper auftreten, sondern als Enabler. Ziel muss es sein, geprüfte und in die bestehende Systemlandschaft integrierte Plattformen bereitzustellen, Schulungen anzubieten und Beratung zu leisten. So können Mitarbeitende befähigt werden, sichere und regelkonforme Anwendungen zu entwickeln, statt im Verborgenen eigene Lösungen zu bauen.

Bevor es zu spät ist

Auch Datenschutz muss von Anfang an mitgedacht werden. Privacy-by-Design, Datenminimierung und klare Zweckbindungen dürfen nicht erst im Nachhinein betrachtet werden. Jede Low-Code-Anwendung sollte dokumentiert, bewertet und regelmäßig überprüft werden. Datenschutz-Folgenabschätzungen können helfen, Risiken frühzeitig zu erkennen und gezielt gegenzusteuern. Letztlich geht es um einen kulturellen Wandel. Unternehmen müssen lernen, Kontrolle nicht durch Verbote, sondern durch Transparenz und Zusammenarbeit zu gewinnen. Wenn Fachabteilungen und IT auf Augenhöhe arbeiten, sinkt die Motivation für Schatten-IT deutlich. So gelingt es, Geschwindigkeit und Sicherheit in Einklang zu bringen und dabei digitale Innovation nachhaltig im Unternehmen zu verankern. Low-Code ist kein Risiko, sondern ein Werkzeug. Die Frage ist nicht, ob Unternehmen es nutzen sollten, sondern wie. Wer klare Strukturen und Integrationen schafft, Verantwortlichkeiten definiert und Sicherheit konsequent integriert, kann das volle Potenzial ausschöpfen, ohne die Kontrolle zu verlieren. Auch für Nutzer entstehen so Vorteile, indem etwa gut integrierte CPMPs für Informationsübertragungen ohne Zeitverlust sorgen.

Über den Autor: Dr. Johann Sell ist Doktor der Informatik. Seit Ende 2022 ist er der Team Lead der Software Entwicklung bei der mip Consult GmbH in Berlin, wo er maßgeblich die Implementierung und Integration leistungsfähiger Consent#Management#Lösungen vorantreibt.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4948750/Low-Code-KI-und-Schatten-IT-Wie-Unternehmen-die-Kontrolle-behalten/