Bei Inhouse-Apps Entwicklern auf die Finger schauen

Apps werden oft von Fachabteilungen direkt bei externen Entwicklern bestellt. Dementsprechend fehlt es oft an strukturiertem Vorgehen über den gesamten Lebenszyklus einer App hinweg. Das kann Probleme in Bezug auf Datensicherheit und Datenschutz verursachen.

DER AUTOR

Philipp Klomp
Gründer und CEO von Nomasis

Firmeneigene (Inhouse-)Apps sind bei mittelständischen und grossen Unternehmen längst zu einem unverzichtbaren Weg für die Abbildung von Geschäftsprozessen geworden. Die Anwendungen reichen von Apps für Business-Software, Verkauf und Customer Relation Management über Marketing- oder Personalprozesse bis hin zu Mitarbeiterumfragen oder Management-Cockpits zur Bereitstellung von Kennzahlen. Anders als bei Apps aus einem öffentlichen App-Store werden Inhouse-Apps nicht durch Apples App-Controlling geprüft.

Die Qualitätssicherung liegt einzig bei den Firmen. Dabei fehlt leider bei vielen Unternehmen eine strukturierte Vorgehensweise für das App-Management über den gesamten Lebenszyklus hinweg. Der Grund dafür ist, dass die Fachabteilungen externe Entwickler direkt mit der Entwicklung der Apps beauftragen. Dies kann nach deren Einführung in Bezug auf Datensicherheit, Datenschutz und Benutzerfreundlichkeit zu gravierenden Problemen führen.

Projekt mit App-Einführung nicht abgeschlossen

Es empfiehlt sich deshalb, mittels eines systematischen Vorgehens das Management von Inhouse-Apps zu planen und zu steuern: Angefangen bei der Definition der Ziele, der Analyse des Ist-Zustands und der Anforderungen über die Konzeption und Realisierung bis hin zum Abschluss inklusive einer Erfolgskontrolle, Dokumentation und der Benennung des weiteren Vorgehens.

Letzterem wird häufig zu wenig Beachtung geschenkt. Nach der Einführung einer App verlangen jedoch Aspekte wie die Entwicklung von zusätzlichen Features oder die Bereitstellung neuer Releases der Betriebssystemhersteller laufend eine eingehende Beachtung durch IT- und Sicherheitsverantwortliche. Die Entwicklung von Inhouse-Apps darf also nicht als Projekt betrachtet werden, das nach dem Rollout abgeschlossen ist.

Nichtsdestotrotz ist in der Regel der Entwickler, häufig ein externer Lieferant, nicht mehr in den Prozess involviert. Der Impact von Upgrades auf die Sicherheit kann indes beträchtlich sein. Ein strukturiertes App-Management muss aber nicht nur weiterführende Massnahmen nach Abschluss eines Projekts beachten. Bereits bei der Konzeption gilt es, Architektur und Prozesse zu identifizieren und insbesondere Richtlinien festzulegen. Diese regeln, wie mit den Herausforderungen an die Security im Hinblick auf die Entwicklung von Apps umgegangen werden soll.

Fachabteilungen und Lieferanten sensibilisieren

Dabei gilt es, eine saubere Vorgehensweise für den App-Management-Prozess zu definieren. Überdies muss sichergestellt sein, dass sich auch der Lieferant Richtlinien zur Sicherstellung eines fehlerfreien Betriebs der Anwendung auferlegt. Denn die Verwendung von Code-Teilen aus Libraries im Internet, etwa für die Einbindung eines PDF-Generators oder ähnlichen Features, kann die Datensicherheit und die Anforderungen an den Datenschutz gefährden. Diese Code-Teile können etwa unbemerkt mit Gefährdern kommunizieren, Angriffe durch Malware auslösen oder Bewegungsprofile der Anwender an Unbekannte weiterleiten.

Zudem gilt zu beachten, dass Inhouse- oder Enterprise-Apps uneingeschränkt Zugang zu Kamera, Mikrophon, Geo- und anderen sensiblen Daten haben. Audits der Lieferanten oder auf Produktebene helfen, dem Schutzbedarf besser gerecht zu werden. Hinzu kommen neue Tools für die automatisierte Sicherheitskontrolle oder für vereinfachten Datenaustausch mit externen Entwicklern, die neue App-Versionen automatisch signieren und mit digitalen Unternehmensschlüsseln versehen. Die Verantwortung für das App-Management obliegt dabei der Firmen-IT. Sie muss beratend auf Fachabteilungen einwirken und alle internen und externen Beteiligten für die weitreichenden Sicherheitsaspekte sensibilisieren.

Illustration: 3moonlight31/shutterstock.com