Praktische Tipps

Kriterien für die Auswahl von Apps

Mit iOS 14.5 müssen Apps transparent angeben, auf welche Ressourcen auf dem Gerät sie zugreifen bzw. welche Berechtigungen sie benötigen. Die Angaben werden von den Entwicklern der Apps gemacht. Daher ist nicht zu 100% garantiert, dass diese Angaben auch stimmen. Trotzdem sollten sie bei der Auswahl von Apps berücksichtigt werden. Das gilt vor allem für Apps, die von Nutzern mit privaten Apple IDs installiert werden. Es gilt auch für Apps, die über das MDM aufgespielt werden. Das BSI gibt weitere nützliche Hinweise, worauf zu achten ist. Die folgenden Fragen orientieren sich daran.

- Wo speichert das App die App-Anwendungsdaten?
  - Speichert es sie auf dem Gerät oder außerhalb des Gerätes?
  - Falls die Speicherung außerhalb Deutschlands oder des EWR erfolgt, könnte das datenschutzrechtlich problematisch sein.
  - Werden vom App personenbezogenen Daten aus der Schule verarbeitet, muss ein Vertrag zur Auftragsverarbeitung mit dem Anbieter bestehen. Ohne diesen ist eine Speicherung auf den Servern des Anbieters nicht zulässig.
- Erfolgt die Speicherung von personenbezogenen Daten auf dem Server des Anbieters (unabhängig, wo dieser steht) automatisch oder kann der Nutzer die Speicherung beeinflussen? (Gefahr eines unkontrollierten Datenabflusses)
- Sammelt das App Nutzerdaten zur Erstellung eines Profils durch Tracker oder Werbung im App?
- Wie sind die Daten im App geschützt? Werden die Daten in der App beim Entsperren der App automatisch entschlüsselt oder können sie mit einem Passwort, TouchID oder FaceID vor unberechtigtem Zugriff geschützt werden?
- Bietet das App eigene Sharing-Dienste oder Netzwerkschnittstellen an?
- Benötigt das App Zugriff auf Daten, die auf dem Gerät gespeichert sind?
- Wird das App durch seine Entwickler regelmäßig aktualisiert?

Es kann für Lehrkräfte sehr hilfreich sein, wenn erfahrene Nutzer in der Schule eine Empfehlungsliste für Apps erstellen, die als gut, sicher und datenschutzkonform nutzbar gelten.

Eine Frage des MDM

Nicht jedes MDM greift alle von iOS bereitgestellten Einschränkungen vollumfänglich auf. Dadurch lassen sich die hier abgegebenen Empfehlungen auch nicht in Gänze umsetzen. Diese Nachteile muss man dann durch umfangreichere organisatorische Maßnahmen ausgleichen. Dazu könnte gehören, dass man die Einschränkungen, welche man nicht durch das MDM vornehmen kann, aber gerne umsetzen möchte, durch die Nutzer vornehmen lässt. Eine entsprechende Schulung und praktische Unterstützung wird dabei in der Regel erforderlich sein.

Schulen, die ihren Lehrkräften die Nutzung von privaten Apple IDs ermöglichen wollen, dabei aber in Bezug auf iCloud auf Nummer sicher gehen möchten, sollten die Anmeldung der Lehrkräfte auf den App Store beschränken, wie oben beschrieben. Die iCloud darf dann nicht aktiviert werden. Damit ist eine sehr sichere Nutzung möglich, da die durch iCloud entstehenden Risiken entfallen.