Digitale Lernräume nutzen: Regeln für die Grundschule

Erstellt von: Anne Frey, behördlich bestellte Datenschutzbeauftragte für die ZfsL der BRK, 10. 5. 2023

Die Handreichungen „Unsere Regeln“ und die „Erläuterungen für die Lehrkraft“ sind als Reaktion auf einen konkreten Fall entstanden.

Der Fall:
Ein Lerntool zur Förderung der Lesekompetenz wird in einer Grundschule eingesetzt. Es bietet auf einer digitalen Lernplattform Texte auf unterschiedlichen Niveaus, dazu Aufgaben sowie eine Auswertung für die Lehrkraft mitsamt Chatfunktion für die Accounts. In einer Klasse tauchten plötzlich im Chatbereich einiger Schüler:innenaccounts Nachrichten auf, die nicht von den jeweiligen Kindern geschrieben worden waren. Zunächst handelte es sich um offenkundige Spielereien: Texte ohne Sinn im Chatbereich, willkürlich „ausgeliehene“ Bücher. Es wurden dann jedoch Bücher „ausgeliehen“ und die zugehörigen Aufgaben ohne Ergebnis geschlossen, wodurch die Punktebilanzen verfälscht wurden. Erst als in einem Account im Chat herabwürdigende und beleidigende Äußerungen an die Klassenlehrkraft auftauchten, informierte ein Kind seine Eltern über diese Nachrichten, die in seinem Namen verfasst worden waren.

Die Dimensionen:
Der Fall bietet Reflexionsräume in unterschiedlicher Hinsicht. Ebenso wie die Frage nach dem erzieherischen Umgang mit dem Verursacher/der Verursacherin sowie der betroffenen Lerngruppe ist die Störung bzw. Entwicklung des Lehr-Lernverhältnisses mitsamt der Rolle der betroffenen Lehrkraft zu bedenken.
Im Kontext Datenschutz ist die fallbezogene Reaktion ebenso interessant wie Prophylaxe. Dies gilt für die Ebene des Systems Schule (Was lernen wir als Grundschule X hieraus?) und für die Ebene des konkreten unterrichtlichen Handelns (Was bieten wir prophylaktisch an?). Das Papier nimmt den Fall vor allem hinsichtlich möglicher Prophylaxen in den Blick.

Die Handreichungen:
Die Handreichungen (Regeln für Klasse 1/2 und 3/4) sowie die Erläuterungen für die Lehrkraft können bezogen auf die eigenen Anwendungsszenarien und Notwendigkeiten adressatengerecht angepasst werden (vgl. Anmerkungen in der Version für die Lehrkraft).
Sie orientieren sich in der vorliegenden Form an den Erfahrungen, die im Kontext dieses Falles in der Kommunikation mit Schule einerseits und dem Anbieter andererseits gemacht wurden. Dem sind z. B. auch die Reihenfolgen der Regeln geschuldet. Besonders relevant erscheint hier eine frühzeitige Reaktion, da die Eskalation sich auch auf die sehr verzögerte Reaktion auf den Missbrauch zurückführen lässt. Eine sinnstiftende Reaktion ist jedoch **nur unter folgenden Voraussetzungen überhaupt möglich:**

- Die Kinder melden Merkwürdiges unmittelbar und nicht erst nach einer Eskalation.
- Die Schule meldet den Vorfall an den/die zuständige Datenschutzbeauftragte/n und erhält Unterstützung bei der Kommunikation mit dem Anbieter, der sich im

vorliegenden Fall zunächst auf den mit der Schule geschlossenen Vertrag zur Verarbeitung von Auftragsdaten (AVV) zurückgezogen hatte.
- Auch die Eltern potentiell betroffener anderer Schüler:innen werden in die Reaktion mit einbezogen (erhalten z. B. Hinweise auf sachgerechte Adressierung ihrer Beschwerde, falls notwendig).

Weiterführende Hinweise: Perspektive Schule, Prophylaxe
Grundsätzlich gilt es, jedes digitale Tool unabhängig vom AVV auf Einhaltung grundlegender Datenschutzregeln zu prüfen. Dies betrifft mit Blick auf den hier betrachteten Fall vor allem das Anmeldeverfahren. Im konkreten Fall kann dieses selbst bzw. die Kommunikation des Anbieters als unangemessen bezogen auf das Risikopotential für die Betroffenen eingeschätzt werden,

- da in der Anmeldung Nutzerkennung und Passwort in einem Kennwort zusammenfasst wurden, welches einer vierstelligen Klassenkennung lediglich eine individualisierte vierstellige Zahlenfolge beifügte (bereits einfaches Ausprobieren ermöglichte die Öffnung weiterer Accounts; eine technische Einschätzung findet sich unten[1]);
- da es die Nutzenden durch die Nomenklatur der Eingabemaske in der Sicherheit wiegt, sie hätten ein Passwort eingegeben (und damit verhindert, dass sie Regeln für eine sichere IT-Nutzung reflektiert erlernen);
- da in den Reaktionen des Anbieters zunächst explizit eine Nichteinhaltung von Standards mit den mangelnden Kapazitäten von Grundschüler:innen erklärt wurde.

Als „To-Do“ bleibt offen, wie Lösungen für eine höherwertige Absicherung insbesondere für den Bereich Grundschule aussehen müssen. In jedem Fall sollte eine Aufweichung von Standards zu Gunsten einer einfacheren Handhabung aufgrund des Alters der Nutzenden vermieden werden. Empfohlen wird die Prüfung einer sinnvollen Passwortverwaltung, zum Beispiel im geschützten individualisierten Bereich des schuleigenen LMS. Bereits Grundschüler:innen müssen lernen, ihre durchaus schon zahlreichen Accounts zu verwalten und dazu geeignete Hilfen zu nutzen. Diese Aufgabe wird umso wichtiger, als die Anzahl der genutzten digitalen Lerntools sich rasant erweitert.

[1] Bei einem Kennwort mit derart geringer Entropie benötigt ein Angreifer bei bekannter Klassenkennung bei 50 Versuchen/Sekunde weniger als 3 Minuten, um mit einem Skript alle Klassenkombinationen durchzuprobieren. Da keine nutzerbezogene Sperrung vorgesehen ist, können unendlich viele Versuche vorgenommen werden. Eine Möglichkeit, Angriffe über zeitliche Anmeldesperren oder die Verweigerung von Anfragen (z. B. bei 20 gescheiterten Anmeldeversuchen/sec) zu verhindern wurde nicht eingebaut.