Liebe Eltern und Erziehungsberechtigten,

hiermit informieren wir Sie gemäß Art. 34 Datenschutz-Grundverordnung (DSGVO) über eine Verletzung des Schutzes personenbezogener Daten.
Nach aktuellem Ermittlungsstand wurden unbefugt Daten kopiert und im Darknet veröffentlicht.

1. Beschreibung des Vorfalls:

Am 15.01.2025 verübte die Hackergruppe LockBit einen Angriff auf die IT-Systeme des IT-Dienstleisters Topackt IT Solutions GmbH, der das Schulnetzwerk „DSNX“ betreibt – auch von unserer Schule genutzt. Wie nun bekannt wurde, sind Daten kopiert und im Darknet publiziert worden.

2. Betroffene Datenkategorien

Nach aktuellem Kenntnisstand könnten folgende Daten betroffen sein:
- Namen, Anschriften und Geburtsdaten von Schüler*innen
- Namen, Anschriften, E-Mail-Adressen und Telefonnummern von Erziehungsberechtigten
- Unterschriften
- Zeugnisse (bis 2022, danach gab es ein neues Zeugnisprogramm)
- Dokumentation zu Fehlzeiten und Verspätungen
- Beurteilungen
- ältere Fotos von Schulfesten oder aus dem Unterrichtsalltag
- Gesundheitsdaten, sonderpädagogische Gutachten, Schwerbehindertenausweise und Ergebnisse schulärztlicher Untersuchungen
- Disziplinarische Maßnahmen
- Schulinterne Vermerke sowie Notizen aus Schulgremien

3. Mögliche Risiken

Der Vorfall erhöht das Risiko für:
- Identitätsmissbrauch
- Phishing- und Betrugsversuche
- Unbefugte Kontaktaufnahme
- Social Engineering (Ausnutzung von Vertrauen, Hilfsbereitschaft, Angst oder Neugier, um Sicherheitsmaßnahmen zu umgehen)
- Erpressungsversuche

Ein Missbrauch der Daten lässt sich nicht ausschließen.

4. Bereits ergriffene Maßnahmen (Art. 33 DSGVO)

Folgende Schritte wurden umgesetzt:

- Isolierung und Sicherung der betroffenen Systeme
- Hinzuziehung externer IT-Forensik- und Sicherheitsexperten
- Meldung an die zuständige Datenschutzaufsichtsbehörde
- Einleitung zusätzlicher technischer und organisatorischer Schutzmaßnahmen
- Prüfung und ggf. Zurücksetzung von Zugangsdaten

5. Empfohlene Schutzmaßnahmen

Wir raten dringend:

- Besondere Vorsicht bei unerwarteten Nachrichten (E-Mail, Telefon, Social Media etc.) – prüfen Sie E-Mails vor dem Klicken auf Links
- Keine Weitergabe sensibler Daten ohne sichere Verifizierung
- Änderung von Passwörtern
- Erhöhte Aufmerksamkeit bei Konto- und Vertragsaktivitäten

Bleiben Sie bitte wachsam gegenüber ungewöhnlichen Mitteilungen, Phishing und Identitätsmissbrauch. Öffnen Sie keine unbekannten Links oder Anhänge und antworten Sie nicht ungeprüft.