

Liebe Erziehungsberechtigte,
liebe Schülerinnen und Schüler,
liebe Kolleginnen und Kollegen,



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

1. Beschreibung des Vorfalls:

Am 15.01.2025 verübte die Hackergruppe Lockbit einen Hackerangriff auf die IT-Systeme des IT-Dienstleisters Topackt IT Solutions GmbH, der das Schulnetzwerk „DSNX“ betreibt, das auch von unserer Schule genutzt wird. Wie jetzt bekannt wurde, sind Daten kopiert und im Darknet veröffentlicht worden. Der Vorfall betrifft auch die Daten der Vorgängerschulen der IGS Rheinzabern, die Realschule und die Hauptschule.

2. Betroffene Datenkategorien

Nach aktuellem Kenntnisstand können folgende Daten betroffen sein:

- Namen, Anschriften und Geburtsdaten von Schüler*innen und Lehrkräften
- Namen und Anschriften von Erziehungsberechtigten
- Kontodaten aus Essensbestellungen
- Unterschriften
- E-Mail-Adressen und Telefonnummern von Schüler*innen, Erziehungsberechtigten und Lehrkräften
- Zeugnisse
- Dokumentation zu Fehlzeiten und Verspätungen
- Beurteilungen
- Schulinterne Vermerke; Interne aus Schulgremien
- Gesundheitsdaten, darunter auch sonderpädagogische Gutachten, Schwerbehindertenausweise, Ergebnisse schulärztlicher Untersuchungen
- Disziplinarische Maßnahmen
- Fotos und Videos

3. Mögliche Risiken

Durch den Vorfall besteht ein erhöhtes Risiko insbesondere für:

- Identitätsmissbrauch

- Phishing- und Betrugsversuche
- Unbefugte Kontaktaufnahme
- Social Engineering (zwischenmenschliche Beeinflussung mit dem Ziel, Personen zu Handlungen zu bewegen, um unberechtigt an Informationen oder in IT-Infrastrukturen zu gelangen. Angreifer nutzen Vertrauen, Hilfsbereitschaft, Angst oder Neugier aus, um Sicherheitsmaßnahmen zu umgehen)
- Erpressungsversuche

Wir weisen ausdrücklich darauf hin, dass derzeit kein konkreter Missbrauch nachgewiesen wurde, ein solcher jedoch nicht ausgeschlossen werden kann.

4. Bereits ergriffene Maßnahmen (Art. 33 DSGVO)

Bislang wurden folgende Maßnahmen 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 (Januar 2025)

5. Empfohlene Schutzmaßnahmen

Wir empfehlen Ihnen dringend:

- Besondere Vorsicht bei unerwarteten Nachrichten (E-Mail, Telefon, Social Media etc.). Prüfen Sie insbesondere E-Mails, bevor Sie darin enthaltene Links anklicken.
- Keine Weitergabe sensibler Daten ohne sichere Verifizierung
- Änderung von Passwörtern
- Erhöhte Aufmerksamkeit bei Konto- und Vertragsaktivitäten

6. Haben Sie Fragen?

Sollten Sie Fragen haben, stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Kontaktieren Sie uns gerne per E-Mail: Datenleak@igs-rheinzabern.de

Ansprechpartner: Ingo Lücking, Andreas Weber, Markus Sabath, Alexander Busse.

Wir bedauern diesen Vorfall außerordentlich. Der Schutz der uns anvertrauten Daten hat für uns höchste Priorität. Wir arbeiten mit Nachdruck daran, die Hintergründe vollständig aufzuklären und unsere Sicherheitsmaßnahmen nachhaltig zu stärken.