Carl-Orff-Realschule plus

Carl-Orff-Realschule plus ✦ Kanalstraße 21 ✦ 67098 Bad Dürkheim ✦ Tel. 06322/95190 ✦ Mail: sekretariat@cor-edu.org

An alle Eltern und Erziehungsberechtigten,
Schülerinnen und Schüler,
ehemalige Schülerinnen und Schüler,
Lehrkräfte sowie aktuelle und ehemalige Beschäftigte unserer Schule

16.03.2026

Benachrichtigung gemäß Art. 34 Abs. 1 DS-GVO über eine Verletzung des Schutzes personenbezogener Daten

Sehr geehrte Damen und Herren,
hiermit informieren wir Sie gemäß Art. 34 Abs. 1 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO) über einen Sicherheitsvorfall, der möglicherweise auch den Schutz Ihrer personenbezogenen Daten betrifft. Zugleich wurde die zuständige Datenschutzaufsichtsbehörde – der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) – gemäß Art. 33 DS-GVO über den Vorfall unterrichtet.

1. Beschreibung des Vorfalls

In der Nacht vom 14. auf den 15. Januar 2025 verschafften sich unbekannte Täter unberechtigt Zugang zu den IT-Systemen eines externen Dienstleisters, der unter anderem für den Betrieb und die technische Verwaltung der schulischen Computernetzwerke mehrerer Schulen in Rheinland-Pfalz zuständig ist. Dabei wurde sogenannte Ransomware (Verschlüsselungssoftware) eingesetzt, die Daten auf Servern verschlüsselt und teilweise unbrauchbar gemacht hat. Auch unsere Schule war von diesem Angriff mittelbar betroffen.
Die Landeszentralstelle Cybercrime der Generalstaatsanwaltschaft Koblenz hat in Zusammenarbeit mit dem Landeskriminalamt (LKA) Rheinland-Pfalz unmittelbar nach Bekanntwerden die Ermittlungen aufgenommen. Nach den bisherigen Erkenntnissen handelt es sich bei den Tätern um professionelle und organisierte Kriminelle.
Unmittelbar nach Bekanntwerden des Vorfalls wurden alle Verbindungen zwischen dem betroffenen Dienstleister und den Schulnetzwerken getrennt. Das betroffene Verwaltungsnetzwerk wurde isoliert und die IT-Infrastruktur schrittweise wiederhergestellt.

2. Aktuelle Entwicklung – Daten im Darknet aufgetaucht

Zunächst war unklar, ob und in welchem Umfang Daten bei dem Angriff tatsächlich abgeflossen sind. Nach jüngsten Erkenntnissen ist nun bekannt geworden, dass vereinzelt Daten aus dem Angriff im sogenannten Darknet – einem verborgenen und nur über spezielle Software erreichbaren Teil des Internets – aufgetaucht sind. Das Landeskriminalamt prüft derzeit den Umfang und Inhalt dieser Daten.
Nach bisherigem Kenntnisstand handelt es sich bei den veröffentlichten Daten in erster Linie um:

- Passwörter und Zugangsdaten von Lehrkräften und Verwaltungspersonal,
- interne Verwaltungsdaten und Verwaltungsdokumente,
- Mustervorlagen und organisatorische Unterlagen.

Es kann jedoch zum gegenwärtigen Zeitpunkt nicht ausgeschlossen werden, dass sich unter den abgeflossenen Daten auch personenbezogene Daten von Schülerinnen und Schülern, Eltern,

Lehrkräften sowie weiteren Beschäftigten befinden. Die abschließende Sichtung und Bewertung der Daten durch die Ermittlungsbehörden dauert an.

3. Möglicherweise betroffene Kategorien personenbezogener Daten

Da der Angriff auf das Schulverwaltungsnetzwerk abzielte, könnten insbesondere folgende Kategorien personenbezogener Daten betroffen sein:

- Name, Vorname, Geburtsdatum, Anschrift,
- Kontaktdaten (Telefonnummer, E-Mail-Adresse),
- Schulbezogene Daten (z. B. Klassen- oder Kurszugehörigkeit, Noten, Zeugnisse),
- Personalverwaltungsdaten von Lehrkräften und Beschäftigten,
- Zugangsdaten und Passwörter für schulische IT-Systeme,
- sonstige in der Schulverwaltung gespeicherte Informationen.

4. Wahrscheinliche Folgen der Datenschutzverletzung

Sollten personenbezogene Daten tatsächlich in unbefugte Hände gelangt sein, bestehen unter anderem folgende Risiken:

- Identitätsmissbrauch (z. B. Eröffnung von Konten oder Abschluss von Verträgen unter Ihrem Namen),
- gezielte Phishing-Angriffe (betrügerische E-Mails oder Nachrichten, die auf persönliche Daten abzielen),
- unbefugter Zugriff auf weitere Online-Konten, sofern identische Passwörter verwendet wurden,
- unerwünschte Kontaktaufnahme (Spam, Betrugsversuche).

5. Ergriffene und geplante Maßnahmen

Zur Eindämmung der Folgen und zum Schutz der Betroffenen wurden bzw. werden folgende Maßnahmen ergriffen:

- Sofortige Trennung aller Netzwerkverbindungen zum betroffenen Dienstleister,
- Isolierung des Schulverwaltungsnetzwerks und Einrichtung einer sicheren Insellösung,
- Zurücksetzung sämtlicher Passwörter und Zugangsdaten der schulischen IT-Systeme,
- enge Zusammenarbeit mit dem Landeskriminalamt, dem CERT des Landes (Computer Emergency Response Team) und der Kreisverwaltung,
- Meldung an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI),
- schrittweise Wiederherstellung der IT-Infrastruktur unter Einhaltung der Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI),
- fortlaufende Überprüfung und Verstärkung der IT-Sicherheitsmaßnahmen.

6. Empfohlene Schutzmaßnahmen für Sie

Wir empfehlen Ihnen vorsorglich, folgende Maßnahmen zu ergreifen, um mögliche Risiken zu minimieren:

- Passwörter ändern: Ändern Sie umgehend alle Passwörter, die Sie im schulischen Zusammenhang verwendet haben. Sofern Sie identische oder ähnliche Passwörter auch für private Dienste (E-Mail, Online-Banking, soziale Netzwerke etc.) nutzen, ändern Sie auch diese.
- Zwei-Faktor-Authentifizierung aktivieren: Aktivieren Sie, wo möglich, die Zwei-Faktor-Authentifizierung (2FA) für Ihre Online-Konten, um den Zugang zusätzlich abzusichern.
- Erhöhte Aufmerksamkeit: Seien Sie in den kommenden Wochen und Monaten besonders aufmerksam gegenüber verdächtigen E-Mails, Anrufen, SMS oder Briefen, die unter

Bezugnahme auf schulische Zusammenhänge persönliche Informationen oder Zahlungen einfordern.
– Keine Links in verdächtigen E-Mails anklicken: Öffnen Sie keine Anhänge und klicken Sie nicht auf Links in E-Mails, deren Absender Sie nicht eindeutig zuordnen können.

7. Ansprechpartner und Kontakt

Für Rückfragen zu diesem Vorfall stehen Ihnen die Schulleitung sowie unser Datenschutzbeauftragter zur Verfügung:

Schulleitung
Telefon: 06322 05190 (über Sekretariat)
E-Mail: sekretariat@cor-edu.org

Datenschutzbeauftragter: Herr Steffen Behrendt
E-Mail: behr@corduew.de
Telefon: 06322 95190 (über Sekretariat, nur Do 7:45 – 9:45 Uhr)

Darüber hinaus können Sie sich jederzeit an die zuständige Aufsichtsbehörde wenden:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34, 55116 Mainz
Telefon: 06131 8920-0
E-Mail: poststelle@datenschutz.rlp.de
Internet: www.datenschutz.rlp.de

Wir bedauern diesen Vorfall sehr und nehmen den Schutz Ihrer Daten äußerst ernst. Sobald uns weitere gesicherte Erkenntnisse vorliegen – insbesondere über den konkreten Umfang der betroffenen Daten – werden wir Sie unverzüglich informieren.

Mit freundlichen Grüßen

A. Walk