Liebe Schülerinnen und Schüler, liebe Eltern, liebe Mitarbeitende, liebe Ehemalige,

liebe Schulgemeinschaft der Elisabeth-von-Thadden-Schule,

wir wenden uns heute mit einem wichtigen Update zu dem bereits im Januar 2025 kommunizierten Sicherheitsvorfall bei unserem rheinland-pfälzischen IT-Dienstleister, der Topackt IT Solutions GmbH, an die gesamte Schulgemeinschaft.

Was passiert ist:

Am 15. Januar 2025 wurden etwa 45 Schulen Opfer eines Hackerangriffs auf das zentrale Schulverwaltungsnetzwerk DSNX, das vom IT-Dienstleister Topackt betrieben und auch von der Elisabeth-von-Thadden-Schule genutzt wurde. Nach Stand der Ermittlungen wurden unbefugt Daten kopiert und verschlüsselt ins Darknet gestellt. Zunächst war nicht klar, ob auch die Elisabeth-von-Thadden-Schule betroffen ist. Dennoch wurde damals sogleich die Schulgemeinschaft informiert und dringend geraten, zur Sicherheit alle schulischen Passwörter zu ändern. Ermittlungen des Landeskriminalamtes (LKA) brachten zunächst keine Hinweise auf eine Veröffentlichung der Daten.

Uns liegen inzwischen neue Erkenntnisse vor:

Seit März 2026 liegen neue Erkenntnisse der Strafverfolgungsbehörden vor. Die Ermittlungsarbeiten durch das LKA und spezialisierte IT-Fachleute haben ergeben, dass im Rahmen eines Cyber-Angriffs einer russischen Hacker-Gruppe neben den veröffentlichten Datensätzen der Stadt Speyer und vieler Schulen in Rheinland-Pfalz auch Datensätze aus dem Verwaltungsnetzwerk der Elisabeth-von-Thadden-Schule im Darknet aufgetaucht sind. Dabei kann es sich auch um personenbezogene und sensible Daten handeln. Hiermit informieren wir deswegen gemäß § 33 Datenschutzgesetz der Evangelischen Kirchen in Deutschland (DSG-EKD) über die Verletzung des Schutzes personenbezogener Daten. Nach aktuellem Kenntnisstand können folgende Daten betroffen sein:

- Namen, Anschriften und Geburtsdaten von Schüler*innen
- Namen und Anschriften von Erziehungsberechtigten
- E-Mail-Adressen und Telefonnummern
- Kontodaten im Zusammenhang mit Essensbestellungen
- Unterschriften
- Zeugnisse
- Dokumentation zu Fehlzeiten und Verspätungen
- Beurteilungen
- Schulinterne Vermerke (z. B. aus Gremien)

• Disziplinarische Maßnahmen

• Gesundheitsdaten (z.B. sonderpädagogische Gutachten, Angaben zu Schwerbehinderungen, schulärztliche Unterlagen)

• Fotos und Videos

Das LKA stellt keine Auswertungen der geleakten Daten zur Verfügung. Personen, die nach Januar 2025 an die Schule gekommen sind, sind von dem Datenzugriff nicht betroffen.

Bitte beachten Sie:

Da der Zugriff auf diese Datenportale hochgradig kriminell und illegal ist, sind wir als Schule und Schulträger vollständig auf die gesicherten Informationen des LKA und des IT-Dienstleisters angewiesen. Wir stehen in engem Austausch, um den Sachverhalt bestmöglich aufzuklären. Uns ist bewusst, dass dieser Vorfall besonders sensibel ist. Daten, die im Darknet veröffentlicht wurden, können in der Regel nicht mehr vollständig entfernt oder kontrolliert werden. Eine Weiterverbreitung durch Dritte kann daher nicht ausgeschlossen werden.

Fakt ist: Wir alle sind als Schulgemeinschaft Opfer eines illegalen Hacker-Angriffs auf unseren IT-Dienstleister geworden und müssen realisieren, dass personenbezogene und sensible Daten abgeflossen sind. Das ist ein schwerwiegender Vorfall, den wir sehr bedauern. Wenn wir nähere Information seitens der Ermittlungsbehörden bekommen, werden wir Sie darüber informieren.

Mögliche Risiken:

Durch den Vorfall kann es zu folgenden Risiken kommen: Identitätsmissbrauch, Phishing- und Betrugsversuche, unbefugte Kontaktaufnahme, social engineering (gezielte Manipulation zur Erlangung von Informationen und Zugriffen), Erpressungsversuche.

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

Was können Sie jetzt tun?

Die schulischen Passwörter wurden im Februar 2025 konsequent geändert. Sollten Passwörter, die damals in der Schule genutzt wurden, auch für private Dienste (E-Mail, social media etc.) verwendet worden sein, sollten diese bitte zur Sicherheit auch dort geändert werden.

Wir empfehlen nachdrücklich: Vorsichtig zu sein bei unerwarteten Nachrichten, keine verdächtigen Links oder Anhänge zu öffnen, keine sensiblen Daten ohne sichere Verifizierung weiterzugeben, sichere, individuelle Passwörter zu verwenden und besonders aufmerksam zu sein bei Konten- und Vertragsaktivitäten.

Sollten Sie in Ihrem Umfeld verdächtige Aktivitäten bemerken, melden Sie sich bitte umgehend.

Was wurde inzwischen getan:

Bereits im Januar 2025 wurde bei der Staatsanwaltschaft Koblenz Anzeige erstattet. Das LKA Rheinland-Pfalz führt das Ermittlungsverfahren. Wichtig zu wissen ist, dass wir gemäß § 32 DSG-EKD bereits im Januar 2025 unsere Aufsichtsbehörde, den Beauftragten für den Datenschutz der EKD, informiert haben. Wir stehen weiterhin in enger Abstimmung mit unserer Datenschutzaufsicht. Im Rahmen Ihrer Betroffenenrechte nach § 16 ff DSG EKD können Sie sich selbstverständlich auch direkt in der Sache an unsere kirchliche Datenschutzaufsichtsbehörde wenden.

Außerdem wurden seit Bekanntwerden des Vorfalls sofort gezielte Maßnahmen ergriffen, um die Daten noch besser zu schützen. Die betroffenen Systeme wurden vom IT-Dienstleister umgehend isoliert und gesichert. Im Zuge der seitdem umgesetzten technischen Erneuerungen und Sicherheitsmaßnahmen wurden an der Schule alle Passwörter erneuert. Anschließend fand ein Penetrationstest durch einen unabhängigen Computersicherheitsdienst statt, um die Sicherheit des schulischen Netzwerkes zu überprüfen. Das alles allerdings kann den erfolgten illegalen Zugriff nicht ungeschehen machen.

Haben Sie Fragen?

Uns ist bewusst, dass dieser Vorfall Fragen aufwirft. Obwohl wir zum aktuellen Zeitpunkt jedoch keine über diesen Brief hinausgehenden Details nennen können, stehen wir Ihnen selbstverständlich für Rückfragen zur Verfügung. Kontaktieren Sie uns bitte per E-Mail unter: datenschutz@thaddenschule.de.

Wir bedauern diesen gravierenden Vorfall außerordentlich und hoffen sehr, dass keine Fälle von Datenmissbrauch vorkommen. Der Schutz der anvertrauten Daten hat höchste Priorität. Für die Schule ist der Vorfall eine Katastrophe. Uns ist deswegen sehr daran gelegen, die Hintergründe vollständig aufzuklären und unsere Sicherheitsmaßnahmen nachhaltig zu stärken.

In diesem Zusammenhang hoffen wir auf Ihr Verständnis und Ihr Vertrauen in dieser schwierigen Situation.

Mit freundlichen Grüßen

OKRin Dr. Silke Dangel

Vorsitzende des Stiftungsrates der Schulstiftung der Evangelischen Landeskirche in Baden als Trägerin der Schule

Dr. Heinz-Martin Döpp

Schulleiter der Elisabeth-von-Thadden-Schule Heidelberg-Wieblingen

Karlsruhe/Heidelberg, den 26.03.2026