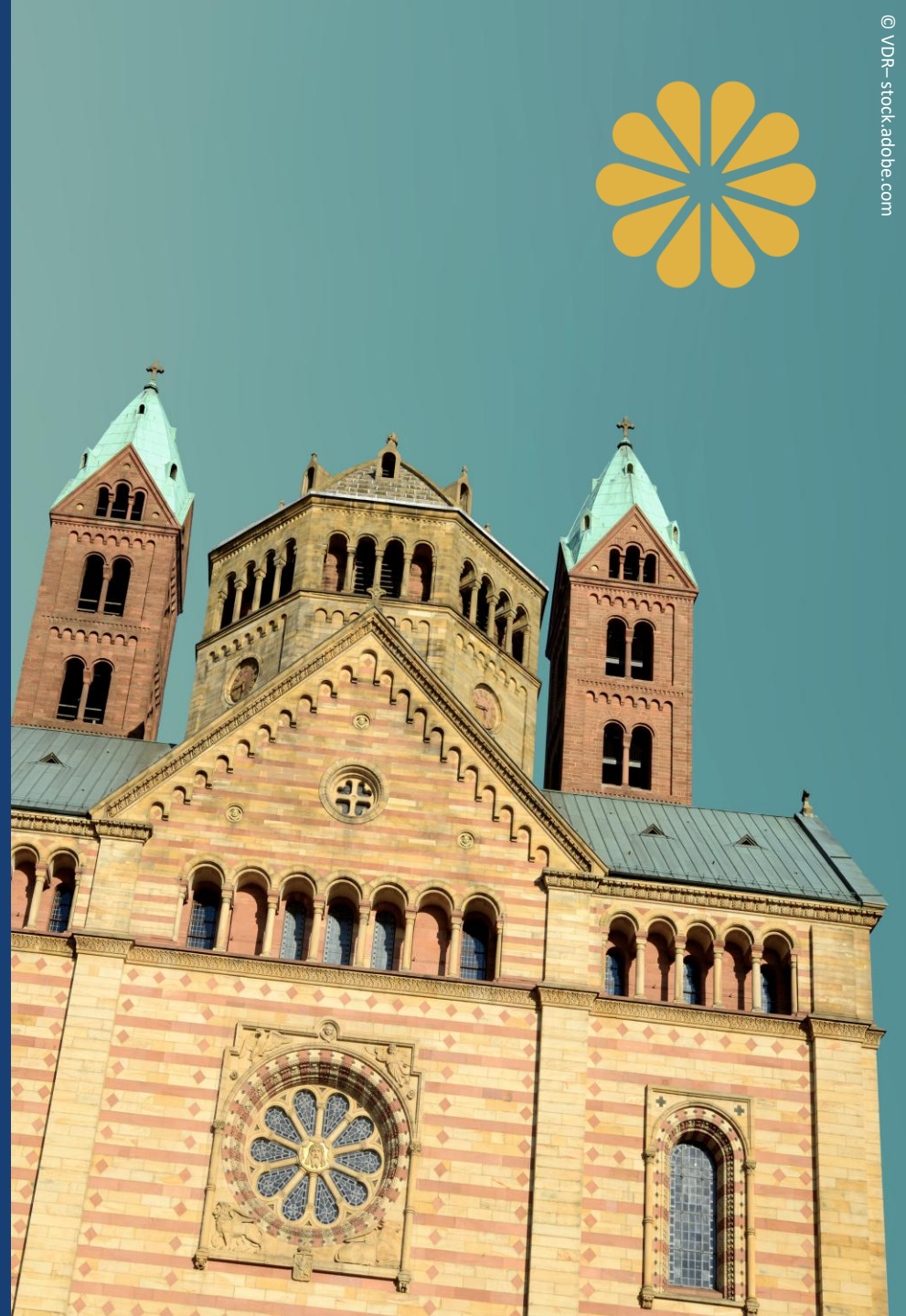
HAUPT-, STIFTUNGS- UND DIGITALISIERUNGSAUSSCHUSS
26. MÄRZ 2026

Cyberangriff vom 15. Januar 2025

SPEYER



WAS IST PASSIERT?
Cyberangriff

- Nacht auf den **15. Januar 2025:** Cyberangriff erkannt
- Morgen des **15. Januar 2025:** städtische EDV-Abteilung trennt alle Verbindungen zu städtischen Schul-Servern
- Weltweit agierende und professionelle Tätergruppe im Bereich Ransomware-as-a-Service
- Zertifizierte Fachfirma sichert Server und säubert Daten
- Daten wurden später im **Darknet** veröffentlicht, Kenntnis darüber am **4. März 2026**

WAS IST PASSIERT?
Infos an die Öffentlichkeit 2025

- **Zeitliche Verzögerung wegen Spurensicherung von ZAC (Zentrale Ansprechstellen Cybercrime)**
- **20. Januar 2025**: Medieninformation der Stadt Speyer
„Hackerangriff auf Schul-IT in Speyer – Untersuchungen dauern an“
- **24. Januar 2025:** Pressemitteilung des Landeskriminalamtes Rheinland-Pfalz und der Generalstaatsanwaltschaft Koblenz *„Pressemitteilung des Landeskriminalamtes Rheinland-Pfalz und der Generalstaatsanwaltschaft Koblenz - Mehrere Schulen in Rheinland-Pfalz von Cyberangriff betroffen*
- **31. Januar 2025**: Medieninformation der Stadt Speyer *„Informationen zu Hackerangriff“*
- **31. Januar 2025**: Einrichtung Bürgertelefon der Stadt Speyer
- **31. Januar 2025:** Aushang durch Abt. 350 – Schule und Sport an alle Schulleitungen
- **29. Oktober 2025:** Sachstandsbericht der Abt. 160 – Schul-IT nach Cyberattacke im Schulträgerausschuss

WAS IST PASSIERT?

Infos an die Öffentlichkeit 2026

- **4. März 2026:** Medieninformation der Stadt Speyer *„Stadt Speyer prüft Situation nach Datenveröffentlichung aus Hackerangriff“*
- **18. März 2026:** Medieninformation der Stadt Speyer *„Aktueller Sachstand zu Datenveröffentlichung aus Hackerangriff“*
- **20. März 2026:** Reaktivierung Bürgertelefon der Stadt Speyer

SPEYER

Rathaus › Medieninformationen › Aktuelle Informationen

Aktueller Sachstand zu Datenveröffentlichung aus Hackerangriff

Die Stadtverwaltung Speyer informiert über den aktuellen Sachstand im Zusammenh
mit der Veröffentlichung von Daten infolge eines Hackerangriffs im Januar 2025.

© Klaus Venus

Nach derzeitiger Einschätzung kann nicht ausgeschlossen werden, dass auch die städtische Kindertagesstätte Schatzinsel von den Datenveröffentlichungen betroffen ist, da diese das Netzwerk der Siedlungsgrundschule zum Teil mitnutzte. Die Information der betroffenen Kinder, Schüler*innen sowie Eltern und Erziehungsberechtigten erfolgt über die jeweiligen Schulen und Kindertagesstätten.

Die Stadtverwaltung steht in engem Austausch mit den zuständigen Behörden und Institutionen, darunter der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, das Landeskriminalamt Rheinland-Pfalz (LKA), das Ministerium für Bildung des Landes Rheinland-Pfalz, die Aufsichts- und Dienstleistungsdirektion (ADD) Trier sowie der beauftragte IT-Dienstleister.

Bei den im Darknet durch die Hackergruppe Lockbit veröffentlichten Daten handelt es sich nach aktuellem Kenntnisstand unter anderem um personenbezogene Daten. Aus rechtlichen Gründen ist es der Stadt nicht möglich, diese Daten selbst herunterzuladen oder zu sichern, da es sich um unrechtmäßig veröffentlichte personenbezogene Daten handelt. Ein Zugriff oder eine Weiterverarbeitung durch die Stadt selbst ist daher nicht zulässig. Die Daten umfassen unter anderem Namen, Anschriften und Geburtsdaten von Schülerinnen und Schülern, E-Mail-Adressen und Telefonnummern sowie schulbezogene Unterlagen wie Zeugnisse, Angaben zu Fehlzeiten und Verspätungen, Beurteilungen und interne Vermerke. In Einzelfällen können auch besonders sensible Informationen, etwa Gesundheitsdaten oder Angaben zu disziplinarischen Maßnahmen, betroffen sein.

Über weitere Entwicklungen wird die Stadtverwaltung fortlaufend informieren. Für Rückfragen wurde ein Bürgertelefon eingerichtet, das unter der Rufnummer 06232 14-1312 erreichbar ist.

Der an die Eltern gerichtete Brief der Stadt Speyer ist **hier** abrufbar.

Medieninformation der Stadt Speyer vom 18. März 2026

WELCHE DATEN KÖNNTEN BETROFFEN SEIN?

- Namen, Anschriften und Geburtsdaten von Schülerschaft und Schulpersonal
- Namen und Anschriften von Eltern-, Sorge- und Erziehungsberechtigten
- E-Mail-Adressen und Telefonnummern von Schülerschaft, Erziehungsberechtigten und schulischem Personal
- Zeugnisse und Leistungsbeurteilungen
- Fotos (z. B. Kollegium, Aktionen, Schulfeste, Bewerbungsfotos, Fotos von Schülerschaft mit erteilten Bildrechten)
- Dokumentation zu Fehlzeiten und disziplinarischen Maßnahmen
- Gesundheitsdaten, darunter auch Gutachten, Schwerbehindertenausweise etc.
- Eventuell Kontodaten
- Ggf. vereinzelte Unterschriften (z. B. von Lehrkräften im eingescannten Elternbrief oder Erziehungsberechtige)
- Schulinterne Vermerke; Interna aus Schulgremien (z. B. Sitzungsprotokolle)
- Daten von Firmen (Berufsbildende Schule)

WELCHE DATEN KÖNNTEN BETROFFEN SEIN?

Mögliche Risiken

- Spam-E-Mails, 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)
- Identitätsmissbrauch und Erpressungsversuche

Es wurde derzeit kein konkreter Missbrauch nachgewiesen, kann aber nicht ausgeschlossen werden.

MASSNAHMEN

Bereits von der Stadt Speyer umgesetzt

- Isolierung der betroffenen Systeme
- Meldung an die zuständige Datenschutzbehörde
- Zurücksetzung aller wichtigen Passwörter sowie Zugangsdaten
- Hinzuziehung externer IT-Forensik- und Sicherheitsexperten
- Einleitung zusätzlicher und organisatorischer Schutzmaßnahmen

MASSNAHMEN

Handlungsempfehlung für die Schulen

- Regelmäßige Änderung von Passwörtern (alle 4 Wochen)
- Besondere Vorsicht bei unerwarteten Nachrichten (E-Mail, Telefon, Social Media etc.)
- Prüfung von E-Mails, vor Öffnen von Links
- Keine Weitergabe sensibler Daten ohne sichere Verifizierung
- Erhöhte Aufmerksamkeit bei Konto- und Vertragsaktivitäten
- Keine Foto-, Video- oder .exe-Anhänge aus offizieller Schule-E-Mail öffnen

NÄCHSTE SCHRITTE

- **Enge Abstimmung** mit Bildungsministerium, ADD (Aufsichts- und Dienstleistungsdirektion Trier) sowie Landesdatenschutzbeauftragte und LKA
- **Transparent informieren** aus diesen Runden
- Weiterhin **Ansprechpartnerin** sein
- Erstellung eines **Leitfadens für Kinder und Jugendliche**

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Fachbereichsübergreifende Arbeitsgruppe:

- Stabstelle 010 – Büro der Oberbürgermeisterin
- Abt. 110 – Hauptverwaltung, Digitale Verwaltung
- Abt. 140 – Recht
- Abt. 160 – EDV
- Abt. 350 – Schule und Sport

Kontakt: sabrina.albers@stadt-speyer.de

SPEYER

www.speyer.de