

Anfrage aus dem Kreistag

eingereicht am:	per Mail am 12.09.2026
zur Beantwortung am:	KT-Sitzung 21.09.2026
Fragesteller:	Herr Riemann
zur Bearbeitung an:	Verwaltung
Termin:	18.09.2026

Anfrage:

Vor dem Hintergrund des Datenvorfalles in Berlin, bei dem rund 5,8 Terabyte Verwaltungsdaten unbemerkt abfließen, frage ich:

Welche technischen und organisatorischen Maßnahmen bestehen im Unstrut-Hainich-Kreis zur Erkennung und Verhinderung eines unberechtigten Datenabflusses sowie zur Wiederherstellung nach einem Cyberangriff?

Wann wurden diese Maßnahmen zuletzt praktisch getestet?

Welche Funktionsträger sind namentlich für IT-Sicherheit, Datenschutz und IT-Notfallmanagement benannt?

Antwort:

1. Welche technischen und organisatorischen Maßnahmen bestehen im Unstrut-Hainich-Kreis zur Erkennung und Verhinderung eines unberechtigten Datenabflusses sowie zur Wiederherstellung nach einem Cyberangriff?

Der Unstrut-Hainich-Kreis verfolgt zum Schutz seiner IT-Infrastruktur und der darin verarbeiteten Daten einen mehrstufigen Sicherheitsansatz. Die eingesetzten technischen und organisatorischen Maßnahmen orientieren sich an den einschlägigen Empfehlungen und Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und werden entsprechend der sich verändernden Bedrohungslage kontinuierlich weiterentwickelt.

Zu den wesentlichen Maßnahmen gehören zum Beispiel die Absicherung und Segmentierung der Netzwerkinfrastruktur, zentrale Sicherheits- und Zugriffssysteme, abgestufte Berechtigungskonzepte.

Ergänzt werden die technischen Schutzmaßnahmen durch organisatorische Regelungen sowie Maßnahmen zur Sensibilisierung der Beschäftigten.

Wesentliche Systeme und Daten werden regelmäßig gesichert. Die Sicherungsstrategie ist so ausgelegt, dass eine Wiederherstellung zentraler IT-Dienste und Daten auch nach Störungen oder Sicherheitsvorfällen ermöglicht werden soll. Aus Gründen der Informationssicherheit können keine weitergehenden Angaben zur konkreten technischen Architektur, zu eingesetzten Sicherheitssystemen, Konfigurationen, Überwachungsmechanismen oder Wiederherstellungsverfahren veröffentlicht werden.

2. Wann wurden diese Maßnahmen zuletzt praktisch getestet?

Die bestehenden technischen Schutzmaßnahmen wurden bereits im Rahmen eines praktischen Testszenarios 2024 / 2025 überprüft. Hierbei wurde ein Cyberangriff simuliert, bei dem sowohl die Verschlüsselung von Client-Systemen als auch der Angriff auf zentrale Datenfreigaben Bestandteil des Tests waren. Im Ergebnis zeigte sich, dass die vorhandenen Sicherheitsmaßnahmen wirksam gegriffen haben und die Systeme des Landratsamtes dem simulierten Angriff standhalten konnten.

Weitere Tests sind in den kommenden Jahren vorgesehen.

3. Welche Funktionsträger sind namentlich für IT-Sicherheit, Datenschutz und IT-Notfallmanagement benannt?

Die Verantwortlichkeiten für Informationssicherheit, Datenschutz als auch IT-Notfallmanagement sind organisatorisch im Landratsamt im Bereich FB4 verortet und namentlich benannt. Notwendige Kontaktinformationen sind über die öffentlich zugänglichen Portale des Landratsamtes einsehbar.