BSZ FÜR GESUNDHEIT UND SOZIALWESEN
Chemnitz | An der Markthalle

Sicherheitsvorfall auf unserer Internetseite www.bsz-gsc.de

Hinweise für Besucherinnen und Besucher

Stand: 14.08.2026

Was ist geschehen?

Unsere Internetseite war Ziel eines unbefugten Zugriffs. Nach dem derzeitigen Kenntnisstand verschafften sich Unbekannte im Zeitraum vom 17. bis 20. Juni 2026 über eine Sicherheitslücke in einer eingesetzten Zusatzsoftware Zugang zum Webserver. Dabei wurde fremder Programmcode eingeschleust, unter anderem in die Menüführung der Seite. Er wurde dadurch beim Aufruf beliebiger Unterseiten an die Browser der Besucherinnen und Besucher ausgeliefert.

Der Vorfall wurde am 6. August 2026 bemerkt. Die Sicherheitslücke ist geschlossen, der eingeschleuste Code wurde entfernt. Aus Sicherheitsgründen wurde die Schulhomepage „offline“ gestellt. Die Schulhomepage wird derzeit grundlegend neu aufgebaut.

Wir bedauern diesen Vorgang und informieren Sie nachfolgend so vollständig, wie es uns nach dem gegenwärtigen Kenntnisstand möglich ist.

Was könnte Besucherinnen und Besucher der Schulhomepage betreffen?

Der eingeschleuste Code hatte die Aufgabe, weitere Inhalte von externen Servern nachzuladen. Diese Inhalte lagen zu keinem Zeitpunkt auf unserem Server.

Was diese externen Server tatsächlich an unsere Besucherinnen und Besucher ausgeliefert haben, lässt sich daher nicht mehr feststellen. Derartige Nachladeadressen liefern erfahrungsgemäß zu verschiedenen Zeitpunkten und an verschiedene Besucher unterschiedliche Inhalte aus.

Die bei uns vorgefundenen Adressen werden in öffentlich zugänglichen Sicherheitsanalysen einer Kampagne zugeordnet, die Besucher betroffener Internetseiten zur Installation von Schadsoftware verleiten soll. Beschrieben werden dabei insbesondere zwei Erscheinungsformen:

- eine Aufforderung, den Browser sei veraltet und müsse sofort aktualisiert werden,
- eine nachgeahmte Sicherheitsabfrage mit der Aufschrift, man möge bestätigen, kein Roboter zu sein.

In beiden Fällen folgt nach der beschriebenen Darstellung die Aufforderung, eine Tastenkombination zu drücken und einen zuvor kopierten Text einzufügen und auszuführen.

Wir können nicht belegen, dass dies auf unserer Seite tatsächlich so geschehen ist. Wir weisen darauf hin, weil wir es nach dem beschriebenen Kenntnisstand nicht ausschließen können und Sie die Möglichkeit haben sollen, Ihr eigenes Gerät zu überprüfen.

Wenn Sie …	**dann …**
unsere Seite lediglich aufgerufen haben	bestehen nach derzeitigem Kenntnisstand keine Folgen für Ihr Gerät.
eine solche Meldung gesehen und weggeklickt oder ignoriert haben	bestehen nach derzeitigem Kenntnisstand ebenfalls keine Folgen.
einer solchen Aufforderung gefolgt sind – insbesondere einen Befehl in Ihr System eingefügt und ausgeführt haben	sollten Sie Ihr Gerät überprüfen lassen.

Ein Befall des eigenen Geräts war nach allem, was zu dieser Vorgehensweise bekannt ist, nur durch aktives eigenes Zutun möglich. Das bloße Aufrufen unserer Seite genügte dafür nicht.

Wichtig: Weder ein echtes Programm-Update noch eine echte Sicherheitsabfrage verlangt jemals, dass Sie einen Befehl aus dem Browser in Ihr Betriebssystem einfügen und ausführen. Eine solche Aufforderung ist immer ein Warnzeichen.

Was können Sie tun?

Falls Sie einer solchen Aufforderung gefolgt sind, dann empfehlen wir Folgendes:

1. Gerät überprüfen – eine vollständige Prüfung mit einem aktuellen Virenschutzprogramm durchführen.
2. Passwörter ändern – möglichst von einem anderen, nicht betroffenen Gerät aus. Vorrangig E-Mail-Zugänge und alle Konten, deren Zugangsdaten im Browser gespeichert waren.
3. Bei Unsicherheit fachkundige Hilfe hinzuziehen.

Allgemeine Hinweise zum Umgang mit Schadprogrammen stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereit: Schadprogramme – Hinweise des BSI

Personenbezogene Daten aus unseren Onlineformularen:

Auf unserer Internetseite wurden ein Kontaktformular sowie ein Formular zur Krankmeldung angeboten. Beides haben wir überprüft:

- Die Formulare speichern die eingegebenen Daten nicht auf dem Webserver. Die Eingaben werden unmittelbar als E-Mail an die Schule übermittelt.

- Eine Veränderung des Formularprogramms selbst konnte anhand der Programmdateien ausgeschlossen werden.

Gleichwohl lässt sich **nicht mit letzter Sicherheit ausschließen**, dass die eingeschleusten Skripte Eingaben aus den Formularen ausgelesen haben, während diese im Browser ausgefüllt wurden. Ein Nachweis hierfür liegt nicht vor; ebenso wenig lässt sich das Gegenteil belegen.

Betroffen sein könnten danach:

- Krankmeldungen, die zwischen dem 17. Juni und dem 3. Juli 2026 über das Formular übermittelt wurden. Danach endete das Schuljahr; das Formular wurde nicht mehr genutzt. Die betreffenden Personen werden von uns gesondert angeschrieben.
- Kontaktanfragen, die zwischen dem 17. Juni und dem 6. August 2026 über das Kontaktformular übermittelt wurden. Übermittelt wurden dabei die von Ihnen angegebenen Kontaktdaten und der Text Ihrer Anfrage.

Sollten Sie in diesem Zeitraum eines unserer Formulare genutzt haben und Rückfragen zu den dabei übermittelten Daten haben, wenden Sie sich bitte an die unten genannten Kontakte.

Was haben wir unternommen?

- Die Sicherheitslücke wurde geschlossen und die betroffene Software aktualisiert.
- Der eingeschleuste Programmcode sowie die abgelegten Schaddateien wurden entfernt.
- Sämtliche Zugänge zur Redaktion der Internetseite wurden zurückgesetzt.
- Der Vorfall wurde der zuständigen Datenschutzaufsicht gemeldet. Wir stehen hierzu in laufendem Kontakt mit dem Datenschutzbeauftragten.
- Die Internetseite wird grundlegend technisch neu aufgesetzt.
- Um Wiederholungsrisiken auszuschließen, wurde die Schulhomepage „offline“ gestellt. Lediglich eine kurze Informationsseite für wichtige Bekanntmachungen ist weiterhin online erreichbar.

Kontakt

Bei Fragen zu diesem Vorfall wenden Sie sich bitte an:

BSZ für Gesundheit und Sozialwesen Chemnitz
An der Markhalle 10
09111 Chemnitz
Tel. 0371/67521-0
info@bsz-gsc.de

Datenschutzbeauftragter
Herr Schmidt, Datenschutzbeauftragter des BSZ für Gesundheit und Sozialwesen Chemnitz
datenschutzbeauftragter@bsz-gsc.lernsax.de