



Stadt Jena • Postfach 10 03 38 • 07703 Jena

Thüringer Landesbeauftragter für
Datenschutz und Informationsfreiheit
Dr. Lutz Hasse
Häßlerstraße 8
99096 Erfurt

Bereich: Büro des Dezernenten
Besucheradresse: Lutherplatz 3
07743 Jena
Zimmer: 318
Telefon: 03641 49-2700
Telefax: 03641 49-2704
E-Mail: Dezernat4@jena.de
Internet: www.jena.de

Ihr Schreiben / Zeichen:
Unser Schreiben / Zeichen:

Datum: 21.01.2019

Vorfall eines gehackten Servers der Jenaer Schulverwaltung

Sehr geehrter Herr Dr. Hasse,

Ende der vorletzten Woche hatten wir in dieser Angelegenheit miteinander telefoniert. Dabei hatte ich Ihnen noch eine schriftliche Stellungnahme zugesagt, die ich Ihnen nunmehr übermitteln möchte.

Die Jenaer Schulverwaltung betreibt neben den Systemen zur Abrechnung und Führung der Schulverwaltung einen Server, auf dem den Jenaer Schulen die Möglichkeit gegeben wird, eigene Webseiten zu betreiben. Dieser Server ist von den Systemen der Schulverwaltung, die auf besonders gesicherten Servern der Stadtverwaltung abgelegt sind, vollständig getrennt.

Auf dem Server für die Internetpräsenz der Jenaer Schulen befinden sich ausschließlich deren selbst erstellte und auch selbst zu pflegende Präsentationen. Diese beziehen sich auf Vertretungspläne, Projekte, Schulfeste usw..

Personenbezogene Daten befinden sich nur insoweit auf dem Server, als dass E-Mail-Adressen oder Namen von Personen beispielsweise im Impressum oder in Präsentationen angegeben werden, die sowieso in die Öffentlichkeit gestellt werden sollten.

Um den 11.12.2018 wurde die Schulverwaltung davon benachrichtigt, dass von diesem Server aus Spam-Mails verbreitet werden. Die Schulverwaltung reagierte sofort, indem der Server und damit die Internetportale der Schulen abgeschaltet wurden. Die Schulverwaltung informierte zeitgleich die Schulen über das aufgetretene Problem und das Abschalten von deren Internetpräsenzen.

Gemeinsam mit dem IT-Bereich der Stadtverwaltung Jena wurde die Ursache der Infektion des Servers gesucht und eingegrenzt:

Viele Schulen nutzen ein veraltetes CMS-System. Bei der Gestaltung einer Fotoprä-



sensation ist mutmaßlich unbewusst ein Plug-in verwendet worden, das infiziert war. Darüber gelang es unlauteren Betreibern, Spam-Mails zu versenden.

Das Schadprogramm wurde gelöscht.

Da nicht zurückverfolgt werden konnte, zu welchem Zeitpunkt das Plug-in installiert wurde, konnten auch die drei Monate zurückreichenden Datensicherungen nicht mehr sicher verwendet werden. Das bedeutete, dass die Schulverwaltung die Seiten alle neu aufbauen musste.

Grundsätzliches:

- Personenbezogene Daten oder der Zugang zu dem Netz der Stadtverwaltung war und ist durch diese Havarie nie gefährdet gewesen.

Der Fehler wurde lokalisiert und beseitigt.

- Zukünftig, da ein erneutes Infizieren grundsätzlich nicht völlig auszuschließen ist, wurde der Server so partitioniert, dass das Infizieren einer Webpräsenz einer Schule nicht auf die von anderen Schulen übergreifen kann.

Für Nachfragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

