

Alephino OPAC – SPAM Warnung

Autor: Frank Bieber

Datum: 09.05.2016

Sehr geehrte AnwenderInnen,

Beim Versenden von Bibliographielisten aus Vollansicht, Listenansicht oder dem Korb mittels „Speichern/Senden“ ist es möglich, Textbestandteile wie „Betreff“ sowie „Überschrift/Anschieben“ individuell zu editieren, wobei Nutzereingaben ggfs. Vorrang vor den hinterlegten Standard-Texten haben. Ebendiese Möglichkeiten wurden von bislang unbekannter Seite offenbar zum Versand unerwünschter Werbebotschaften und somit mißbräuchlich eingesetzt. Daß auf die beschriebene Weise lediglich der Text-Vorspann von aus Alephino generierten Bibliographielisten manipuliert werden kann, das Ganze mithin sehr eigenwillig aussieht, stört die Angreifer offenbar nicht.

Die Gefahr des Mißbrauchs ist stets dann gegeben, falls Ihr von unserem OPAC genutzter Mail-Server die Weiterleitung von Nachrichten an beliebige Adressaten zuläßt.

Die vorgenannten SPAM-Angriffe lassen sich durch nachfolgende beschriebene Änderungen der Konfiguration des OPAC ausschließen. Gehen Sie hierzu wie folgt vor:

1. Bearbeiten der Konfigurationsdatei des OPAC **etc/alipac.cfg**:

(MailAuth) HideParams=Y ← diese Parameterzeile einfügen
--

2. Entfernen der nunmehr unwirksamen Eingabefelder „Betreff“ und „Überschrift/Anschieben“ aus dem(n) eMail-Formular(en) des OPAC durch Entfernen oder Auskommentieren der markierten Abschnitte in den Datei(en) **htdocs/alipac_[lang]/save-mail-form.htm**:

```
<tr>
  <td class="td2">Kodierung</td>
  <td class="td2">
    <input TYPE="radio" NAME="CHARSET" VALUE="" checked>UTF-8
    <input TYPE="radio" NAME="CHARSET" VALUE="EXTTOISO">ISO Latin-1
  </td>
</tr>
</tr>
<!--
<tr>
  <td class="td2">Betreff</td>
  <td class="td2"><input size=40 name="SUBJECT" value=""></td>
</tr>
-->
<tr>
  <td class="td2">E-Mail</td>
  <td class="td2"><input size=40 name="EMAIL" value=""></td>
</tr>
<!--
<tr>
  <td class="td2">&Uuml;berschrift/<br>Anschreiben</td>
  <td class="td2">
    <textarea name="HEAD" cols=30 rows=2></textarea>
  </td>
</tr>
-->
```