Security

My server sends spam, what can I do about it?

1. The server is hacked - in this case the sender has access to your server and can send the e-mails directly or via a script. You can detect this with tools like Chkrootkit. The only way to make sure that the hacker has no access to your server is to reinstall it. First you should change the passwords to your mail accounts.
2. The mail server works as an open relay - in this case the mail server accepts every e-mail without authentication and sends it on. Since our basic configuration is designed so that authentication is always required, this also indicates that the server has been hacked or that you have changed the configuration of the mail server accordingly. This vulnerability can be tested e.g. on the following page: http://www.mailradar.com/openrelay/
3. The sender uses cross site scripting - in this case the attacker uses an incorrectly programmed web page / CMS on your server to execute a script. Cross site scripting can be detected by connecting the log files of the mail server and the web server. In this case an e-mail must have been sent by the user wwwrun or www-data and at the same time in the log file of the web server a web page must have been called. By evaluating this call, both the relevant script on the server and the downloaded script of the attacker can be identified and the IP of the calling server determined.
   Further information about Cross Site Scripting http://de.wikipedia.org/wiki/XSS.
   General server security information http://www.bsi.de.

Unique solution ID: #1434
Author: Bettina Brauer
Last update: 2021-04-01 06:25