Security

How can I tell if my server has been hacked / compromised?

This question is very difficult to answer. In extreme cases this is not recognizable at all or only with special analysis tools.

Unusual behavior of your server can be a sign, but it does not have to be. An increase in the amount of undeliverable emails sent back can be an indication that your server is being misused to send spam emails. The same phenomenon occurs, however, when someone uses the server address as the sender address to outwit an existence check of the sender domain. In the latter case, your server has nothing to do with the sending, but receives all emails returned as undeliverable.

A sure sign that an unauthorized person has tampered with your server is always the disappearance of log files or the modification of data.

If you suspect that an intruder has tampered with your system, checking the log files or using a test program usually helps. These programs usually search for so-called rootkits You can find more information on this at http://de.wikipedia.org/wiki/Rootkit.

The proven testing tools are Windows Blacklight (available at: http://www.f-secure.com/blacklight) and Linux checkrootkit (available at: http://www.chkrootkit.org).

A well-maintained list of current security vulnerabilities can be found at http://www.securityfocus.com/ under Bugtraq. If you want general information about computer security, we recommend the BSI Grundschutzhandbuch, which you can download free of charge at https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

Unique solution ID: #1435
Author: Bettina Brauer
Last update: 2021-04-01 06:28