Скрипт очистки почтовой очереди

Опубликовано muff в Пт, 2011-12-23 02:49

Случилась незадача... У одного из пользователей почтового сервера "своровали" параметры подключения к почтовому серверу (скорее всего с помощью троянца какого-то). Пользователю была разрешена отправка сообщений через СМТП-авторизацию. Злоумышленники воспользовались этой возможностью и организовали рассылку.

Реквизиты доступа изменены в первую очередь, однако в почтовой очереди сообщений еще тысячи нелегитимных сообщений от этого пользователя. Очищать всю очередь сообщений - не вариант. Так можно и полезных сообщений лишиться. Удалять сообщения по одному - это тоже не вариант. Необходимо поставить это дело "на конвеер". Помочь в этом может следующий скрипт:

```
#!/bin/sh

exim -bp | grep user [at] domain [dot] com |
        (
                while read ID
        do
                        IDGOOD=`echo $ID |awk '{ print $3 }'`
                if [ -n "$IDGOOD" ]; then
                        exim -Mrm $IDGOOD
                 fi
        done
)
```

где user [at] domain [dot] com - почтовый адрес, от которого выполнялась рассылка.

Медленно, но уверенно скрипт выполняет свое дело. Для ускорения процедуры можно запустить скрипт в несколько потоков, тоесть несколько раз. В таком случае необходимо внести изменения в скрипт и для вывода сообщений воспользоваться командой **exim -bpr**

Источник (получено *2025-06-03 18:39*):
http://muff.kiev.ua/content/skript-ochistki-pochtovoi-ocheredi