

Памятка: что сделать после взлома сайта

Сайт вычистили. Дальше – восемь шагов, которые остаются за владельцем и его программистом. Распечатайте и отмечайте сделанное.

Чистка не защищает от повторного взлома. Если не закрыть то, через что вошли, злоумышленник вернётся тем же путём. Поэтому шаги ниже – не «по желанию».

1 Сменить все пароли

Считайте украденным всё, до чего взломщик мог дотянуться, а не только пароль администратора сайта.

- | | |
|--|---|
| ☐ администраторы сайта (1С-Битрикс, WordPress и другие системы) | ☐ панель управления сервером |
| ☐ FTP, SFTP, SSH | ☐ почта администраторов |
| ☐ личный кабинет хостинга или сервера | ☐ учётные записи разработчиков, у которых был доступ |
| ☐ база данных | ☐ ключи и токены для обмена с другими системами |

До смены выпишите, где эти пароли и ключи прописаны: обмен с 1С, CRM, оплата, доставка, почта сайта. После смены впишите туда новые – иначе обмен остановится.

2 Проверить пользователей сайта

- | | |
|---|---|
| ☐ удалить незнакомых пользователей | ☐ проверить группы и права |
| ☐ сверить список администраторов | ☐ убедиться, что не осталось скрытых учётных записей |

3 Проверить доступы к серверу

Это работа для программиста или администратора сервера.

- | | |
|--|--|
| ☐ SSH-ключи: нет ли чужих | ☐ подозрительные процессы |
| ☐ пользователи FTP и SFTP | ☐ лишние учётные записи на хостинге |
| ☐ задачи по расписанию (cron) | |

4 Обновить всё, что установлено

- | | |
|---|---|
| ☐ ядро сайта (1С-Битрикс, WordPress) | ☐ шаблон |
| ☐ PHP | ☐ сторонние компоненты |
| ☐ модули, плагины, расширения | |

Если в стороннем модуле или шаблоне есть известная уязвимость – поставить свежую версию или закрыть уязвимость другим способом.

5 Настроить резервные копии

- ☐ копия делается сама, каждый день
- ☐ копируются несколько версий, а не одна последняя
- ☐ копии лежат отдельно от сервера сайта
- ☐ раз в несколько месяцев – пробное восстановление из копии

Файл backup.zip – ещё не резервная копия. Копия есть только тогда, когда из неё удалось поднять сайт.

6 Защитить учётные записи

- ☐ вход администраторов с кодом из приложения или СМС (двухфакторная защита)
- ☐ доступ в админку только с нужных адресов
- ☐ у каждого свой логин вместо общего admin
- ☐ каждому – только те права, которые нужны для работы

7 Наблюдать первые недели

Если что-то из списка появилось снова – вход остался открыт.

- ☐ подозрительные файлы
- ☐ новые пользователи
- ☐ изменения в файлах сайта
- ☐ незнакомые задачи по расписанию
- ☐ переадресация на чужие адреса
- ☐ всплески нагрузки
- ☐ рассылка спама с сайта
- ☐ новые страницы и ссылки в поиске

8 Записать, что произошло

Пригодится при повторном случае, смене подрядчика и для вопросов от клиентов.

Когда обнаружили

Что именно обнаружили

Что сделали

Какие доступы могли быть украдены

Какие пароли сменили

Какие уязвимости закрыли

Дата последней проверки
