Чек-лист безопасности сайта

1. Всегда имейте под рукой резервную копию данных. Лучше несколько резервных копий. Самое страшное — потеря ключевых данных. В такой ситуации отсутствие бэкапа — катастрофа.

2. Если ваш сайт использует готовый движок — регулярно обновляйте его. А заодно темы сайта, плагины и вообще всё, что не было разработано непосредственно для вас.

3. Не используйте для сайта компоненты, скачанные не с официального сайта/репозитория разработчика. Мало кто делает code review для компонента, который скачал на сайте лучшие-бесплатные-плагины-точно-без-вирусов.рф

4. Всегда используйте безопасные пароли: от 8 символов, разный регистр, спецсимволы. Пароли вида Admin12345 взламываются брут-форсом по словарю за 5-10 минут.

5. Если ваш сайт использует готовый движок, найдите рекомендации по безопасности. Поиск и реализация — 30 минут работы, закрыть извне доступ к системным папкам сайта — бесценно. Используемые плагины можно проверить в трекерах публично известных уязвимостей:

   wpvulndb.com — для Wordpress
   vel.joomla.org — для Joomla
   drupal.org/security — для Drupal

6. Если есть возможность, используйте WAF — Web Application Firewall, модуль или плагин на сайте, который блокирует подозрительные запросы.

7. Обязательно ведите логи запросов к сайту — да, это несколько увеличивает нагрузку на дисковую подсистему, но позволяет обнаружить попытки взлома, брутфорса или сканирования на предмет уязвимостей.

8. Если у вас больше одного проекта, размещайте их под разными пользователями. Так вы снизите вероятность перекрестного заражения.

9. Если ваш сайт использует язык PHP, попросите разработчика или системного администратора отключить потенциально опасные функции (конечно, если они не используются на сайте). Обычно это exec, passthru, shell_exec, system, proc_open, popen, curl_exec, curl_multi_exec, parse_ini_file, show_source

Если сайт заразили:

Лучше всего обратитесь к специалисту (своему или стороннему). Если у вас нет опыта, устранять последствия самому будет сложно и долго. В крайнем случае можно восстановить файлы сайта из резервной копии, сделанной до заражения.

Когда устранили заражение:

Попробуйте зафиксировать точку заражения по логам доступа сайта. В большинстве случаев следует искать POST-запросы большого объёма или прямое обращение к файлам тем/модулей.

Если точку заражения обнаружить не удалось, пройдитесь еще раз по пунктам 1-9. Как минимум поменяйте пароли.

Если сайт на готовом движке, проверьте его темы/плагины в публичных базах данных уязвимостей. Найдёте — нужно запатчить силами разработчика/обновления уязвимого компонента.

Советы подготовили в FirstVDS.ru

Невредные советы

для здоровья сайта

01 Настройте бэкап

Резервная копия сайта — ваш «спасательный круг» на случай любых форс-мажоров. В любой момент времени вы сможете запустить работающий сайт из бэкапа.

02 Проверьте бэкап

Убедитесь, что бэкапы работают корректно и сохраняют нужные данные. Для этого разверните копию сайта на сервере — например, на поддомене.

03 Повторите пункт 01

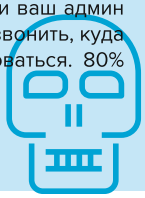
История знала случаи потери данных в облачных хранилищах, у хостеров, на личных жестких дисках. Но не потерю данных сразу везде. Храните бэкапы в разных местах.

04 Спланируйте шаги

Создайте план по восстановлению работоспособности сайта. Лучше, если планов будет несколько: когда упал сервер, дата-центр, интернет в половине мира. Предел — только ваш пессимизм.

05 Учебная тревога!

Сформируйте набор инструкций для восстановления на случай, если ваш админ будет в отпуске, больнице или недоступен по другой причине. Кому звонить, куда писать, какие инструкции отправлять и на какие сроки ориентироваться. 80% аварий переносятся намного легче, когда есть **contingency plan**.



06 Настройте мониторинг внутри и снаружи

Настройте мониторинг важных параметров на сервере: нагрузки, дискового пространства, свободной памяти, состояния процессов. Можно использовать готовые решения мониторинга (Munin, Zabbix, etc). Проверяйте состояние сайта извне, как минимум через Google и Яндекс. Внутри сервера всё может быть в порядке, а с доступностью или скоростью — проблемы.

07 Будьте начеку

Настройте моментальные уведомления о критичных проблемах: не работает сайт, кончились ресурсы. Уведомления обо всех некритичных проблемах — в рабочее время.

08 Тестируйте всё

Проверьте работу мониторинга, запустив несколько тестовых аварий. Например, заполните диск, погасите сайт в момент минимального трафика. Нужно знать, что аварии будут зафиксированы.

09 Не экономьте на ресурсах

Проверяйте хотя бы раз в квартал, хватает ли ресурсов сервера под нужды проекта. Можно проводить нагрузочные тестирования или проверять использование ресурсов по мониторингу. При необходимости оптимизируйте настройки сервера. Состояние любого проекта динамическое, и настройки, сделанные полгода назад, могут не подходить под текущее состояние сайта.

10 Готовьте сани летом

Перед плановым ростом трафика (реклама, сезонные акции) делайте нагрузочное тестирование. Ситуация, когда на сайт пустили рекламу, а он падает из-за нехватки ресурсов, печалит любого маркетолога :(

11 Не затягивайте

Если нагрузка внезапного возросла (об этом сообщит мониторинг из пункта 6), а трафик нет — свяжитесь с вашими админами. Это может быть признаком атаки на сайт, внезапной деградации оборудования и прочих неприятностей.

Поможем и подскажем.

FirstVDS.ru