Отчет по сайту marsel-shapkioptom.ru

23/01/2020

Сайт просканирован на наличие всех видов хакерских скриптов, вредоносного кода и вирусов, вылечен, установлена защита от веб-атак.

> Пожалуйста, внимательно ознакомьтесь с отчетом, так как он содержит важную информацию о безопасности сайта, доступе в панель администратора и гарантийном обслуживании.
>
> Выполните пункты из раздела **”Что осталось сделать”**, чтобы сайт оставался неуязвимым для хакерских атак.

В конце отчета приведен инструктаж по технике безопасности, который важно соблюдать для того, чтобы работа с сайтом была максимально безопасной.

ⓘДля тех, кто обновляет и администрирует сайт:
Если потребуется изменить/обновить плагины или CMS, перенести сайт на другой хостинг или внести изменения в шаблоны (файлы), используйте инструкцию по ссылке https://revisium.com/ri/ и ознакомьте с ней сторонних специалистов, которые будут вносить изменения на сайтах, чтобы защита была постоянно активна.

Revisium
Лечение и защита сайтов

Перечень выполненных процедур нашими специалистами

1. Файлы сайта, база данных и страницы сайта просканированы на все виды вредоносного кода, вирусов и хакерских скриптов.
    - Обнаружены и удалены хакерские скрипты и вставки вредоносного кода в следующих файлах:
        - admin/image.php
        - admin/infodata.php
        - catalog/image.php

2. Доступ к административным функциям и разделам CMS защищен двухфакторной аутентификацией с помощью дополнительного пароля.

   Данная мера закрывает ряд уязвимостей в панели управления, административном каталоге и не позволяет получить несанкционированный доступ к админ-панели сайта злоумышленнику, даже если он перехватит или украдет логин и пароль от CMS.

   При входе в панель администратора сайта откроется страница дополнительного пароля, в который нужно ввести:

   `larobiri98`

   Далее откроется стандартная страница входа администратора – используйте ваши старые логин и пароль для входа в административную панель.

3. На сайтах установлена проактивная защита, блокирующая веб-атаки хакеров и ботов, несанкционированный доступ в админ-панель и к служебным файлам. Проактивная защита выполняет также функцию расширенного мониторинга и сохраняет информацию о веб-запросах (в том числе содержимое POST запросов) в специальный журнал, что позволяет при возникновении инцидентов безопасности провести детальный аудит.

   Установленная **проактивная защита** обладает следующими возможностями:
   - блокирует опасные запросы по http от ботов и хакеров
   - выполняет виртуальный патчинг уязвимостей скриптов CMS и защищает от:
       - удаленного выполнения кода (RCE),
       - локального и удаленного включения файлов (LFI/RFI)
       - SQL инъекций
       - инъекций контента в страницы
       - несанкционированной загрузки произвольных скриптов (AFU)
       - несанкционированного размещения спам-материалов и автопубликации спам-страниц
       - спама форм обратной связи и регистрации (при включенной защите от http флуда)

         и других видов уязвимостей и веб-атак на сайт.
   - блокирует брутфорс-атаки и выполняет защиту от http флуда

- ограничивает несанкционированный доступ к служебным каталогам и скриптам
- позволяет ограничивать по IP доступ к страницам, блокировать по IP опасных ботов и вредоносные запросы
- позволяет добавлять безопасные HTTP заголовки при генерации страниц
- фильтрует запросы от недобросовестных веб-сервисов и опасных ботов
- сохраняет запросы к сайту в журнале мониторинга

Проактивная защита подключена в параметре php auto_prepend_file как скрипт из каталога lor_protect/lor_o.php.

[1] Для проверки работы проактивной защиты перейдите по ссылке:

- **https://marsel-shapkioptom.ru/?bd524144c36a90cb8f9574a47725474a**

  Если на странице вы видите

  Web Protection (WAF) – OK
  Files – OK

  то защита активна. Если второй пункт красный или выдается обычная страница сайта, то защита не работает на 100% или полностью отключена.

[2] Мы рекомендуем регулярно менять пароли. Поэтому, чтобы **в будущем** установить новый пароль от административных разделов, воспользуйтесь инструкцией https://revisium.com/ri/#q7. Для получения нового пароля, перейдите по ссылке:

- **https://marsel-shapkioptom.ru/?lor_secret=bd524144c36a90cb8f9574a47725474a**

Строку зеленого цвета сохраните в надежном месте (это будет ваш новый пароль), а синюю строку нужно разместить вместо текущего содержимого в указанном ниже файле (после этого новый пароль станет рабочим, а старый – работать перестанет):

- /var/www/vh224654/data/www/lor_protect/htpasswd/htpasswd.2036855346c1477aaada1b520828cdd3

(данный файл доступен через файловый менеджер хостинга или SFTP подключение в программе FileZilla или WinSCP5)

4. Проактивная защита позволяет смотреть статистику атак, заблокированных запросов, он-лайн запросы, географию запросов и другую статистику за последний месяц. Ссылка на административную панель проактивной защиты:
   - **https://marsel-shapkioptom.ru/?lor_ui=bd524144c36a90cb8f9574a47725474a**

5. На сайте установлено “цементирование” сайта.
   Данный элемент защиты исключает несанкционированные изменения файлов скриптами. Подробно о данной защите можно прочитать на странице

http://revisium.com/ru/clients_faq/#q4, в частности выполнены следующие операции:

- в корневом .htaccess размещены правила, блокирующие веб-атаки;
- изменены права на файлы и каталоги на более безопасные;

Что осталось сделать

1. Проверьте основные функции сайта (страницы основных разделов, формы обратной связи, функции админ-панели и добавление товара в корзину, если это интернет-магазин), а затем **через сутки** сделайте резервную копию через панель управления хостингом, чтобы, в случае проблем, восстановить сайт из проверенной резервной копии. При создании архива важно сохранить атрибуты файлов и каталогов, поэтому простое копирование файлов по FTP в данном случае не подойдет. Лучше всего для этого подходит резервное копирование в панели хостинга, где можно загрузить новую резервную копию вылеченной версии сайта и базы данных.

   Как это сделать правильно, уточните в тех поддержке хостинга или справочном руководстве по панели хостинга.

2. Смените пароли: от FTP, от SSH, от панели управления хостингом и административной панели сайта.
   (Данный пункт является обязательным для сохранения гарантии на нашу работу)

   Пароли должны быть сложными, например **djdWe3#csdj@ker**
   (для удобства мы сделали генератор паролей https://revisium.com/tools/ht.php).

Памятка безопасности

Что нужно сделать сразу после получения отчета

- Выполните рекомендации из раздела “Что осталось сделать”
- Очистите кэш браузера и куки перед открытием сайта после лечения
- Рекомендуем добавить сайт в панели веб-мастеров Google (http://www.google.com/intl/ru/webmasters) и Яндекс (http://webmaster.yandex.ru). В этом случае Вы своевременно будете информированы об изменениях, происходящих с сайтом. В том числе, касающихся безопасности.
- Проверьте свой рабочий компьютер коммерческим антивирусом (например, Антивирусом Касперского или Dr.Web)
- Если с вашим сайтом работает сторонний специалист, он также должен проделать все перечисленные действия, ознакомиться с данной памяткой, следовать ее рекомендациям постоянно.

Что нужно делать регулярно

Внимание, данные действия нужно выполнять как владельцу сайта, так и сторонним специалистам, которые работают с сайтом.

- **Обеспечьте безопасность своего рабочего места:** работайте с компьютера, защищенного коммерческим антивирусом с обновляемыми

вирусными базами, и регулярно проводите полную проверку рабочего компьютера.

- **Обеспечьте безопасность интернет-подключения:** если с сайтом работаете не из дома, подключайтесь с помощью VPN. Не работайте с сайтом через публичные WI-FI.
- **Следите за обновлением версии CMS вашего сайта**. Регулярно обновляйте CMS и плагины, если это возможно.
- **Проверяйте работу защиты с помощью ссылки из пункта №2** (должно быть два зеленых пункта)
- **Регулярно загружайте полную резервную копию сайта (файлы и базу данных)** локально на ваш компьютер. Не стоит на 100% полагаться на резервное копирование хостинга. Если у вас выделенный сервер (VPS), не забудьте включить резервное копирование.
- **Проверяйте сайт сканерами ReScan.Pro и AI-BOLIT.**

Что не нужно делать, так как из-за этого сайт могут взломать

- Не храните пароли в браузере и FTP клиенте, это опасно. Используйте менеджеры паролей.
- Не пользуйтесь FTP, пользуйтесь безопасной альтернативой – SFTP или хотя бы FTP через защищенное подключение FTPS. В тех поддержке хостинга можно уточнить, как подключаться по SFTP.
- Не отдавайте полные доступы сторонним специалистам (фрилансерам и субподрядчикам), каждому нужно создавать отдельный, ограниченный и временный аккаунт перед началом работ, а по завершении работ сразу поменять пароль или удалить аккаунт.
- Не отключайте защиту более чем на сутки.
- Не устанавливайте нелицензионные плагины, шаблоны и модули, загруженные из непроверенных источников.
- Не работайте с сайтом из публичных (открытых) WI-FI сетей (в метро, парках, отелях), так как доступы могут перехватить и взломать сайт. И предупредите об этом сторонних специалистов, которые будут работать с вашим сайтом. Используйте VPN подключение или хотя бы подключение через 3G/LTE (телефон/модем).
- Не размещайте на аккаунте хостинга новые сайты, если они не были проверены на вредоносные скрипты специалистами и на них нет защиты от взлома.

Что делать в случае возникновения проблем с сайтом

Если все наши рекомендации по безопасной работе с сайтом выполнены, то сайт будет защищен от веб-атак и хакеров. Тем не менее, если вы обнаружите взлом или вирус на сайте, необходимо выполнить следующие действия незамедлительно:

1. Запросить в тех поддержке журнал веб-сервера (файлы access_log и error_log) и журналы FTP/SFTP подключений и операций с файлами за максимально доступный период.

2. В случае спам-рассылки с сайта запросить в тех поддержке образцы рассылаемых писем (важна дата, время рассылки и служебный заголовок писем)
3. Прислать нам на audit@revisium.com доступы к хостингу, описание возникшей проблемы (как, что и когда было обнаружено) и данные из пунктов 1 и 2.

Не восстанавливайте сайт из резервной копии и не пытайтесь устранить проблему самостоятельно, это не даст возможность провести аудит и выяснить причину.
Мы выполним анализ и устранения самостоятельно в рамках гарантийной поддержки.

Гарантийное обслуживание

В случае повторного взлома/заражения в рамках гарантийной поддержки, мы обязуемся бесплатно вылечить сайт и закрыть уязвимость, если условия гарантии сохранены.

Гарантийное обслуживание сайта оказывается только при выполнении всех рекомендаций, перечисленных в “Памятке безопасности”. Если какие-то рекомендации не будут выполнены, сайт останется уязвим, и в этом случае мы не сможем гарантировать его безопасность. Поэтому просим Вас выполнить все пункты и проинформировать нас об этом по email audit@revisium.com .

Снятие защиты с сайта (изменение прав на файлы и директории), перенос на другой хостинг или аккаунт без сохранения защиты, а также открытие админ-панели CMS для всех (без дополнительной авторизации) делает сайт уязвимым, в этом случае сайт также снимается с гарантийного обслуживания, а лечение и установка защиты в случае возможных проблем, будет предложена на платной основе.

При обращении, пожалуйста, пришлите нам на audit@revisium.com подробное описание проблемы и доступы к хостингу и в админ-панель CMS.

Вопросы и ответы

Если у вас появились вопросы по защите сайта или отчету, пожалуйста, посмотрите наш закрытый клиентский раздел “Часто задаваемые вопросы”

http://revisium.com/ri/

Благодарим Вас за обращение к нам.
Безопасной работы в сети!

Информацию по безопасности сайта можно найти на страницах

https://vk.com/siteprotect

https://facebook.com/revisium

https://twitter.com/revisium

https://revisium.com/kb/

https://t.me/sitesecurity (Телеграм канал)

С уважением,
команда “Ревизиум”.