Приложение

Методические рекомендации по основам безопасной работы с сайтами, размещенными на хостинге 68edu.ru.

При работе с сайтами, размещенными на хостинге 68edu.ru, необходимо обращать внимание на следующее:

1. Скачивайте плагины и шаблоны только с надежных и проверенных сайтов. Не устанавливайте те приложения, в которых Вы не уверены, особенно, если Вы нашли бесплатный шаблон, который должен быть платным.

2. Пароль на административную часть должен быть сложным, содержать специальные знаки (!@#$%^_&), разный регистр букв (aA), включать в себя цифры и должен быть длиною минимум в 8 символов.

3. Ваша антивирусная программа должна быть актуальной, регулярно обновляться, при этом не забывайте запланировано 1 раз в неделю запускать антивирусную программу для проверки компьютера и USB-накопителя на содержание вирусов. Есть программы-роботы, следящие и запоминающие, что Вы вводите с клавиатуры, при этом составляется база наиболее часто встречаемых слов, из этой базы впоследствии в первую очередь будут подбираться пароли.

4. Не храните пароли от сайта в панели мастера паролей Вашего браузера, это облегчает взлом сайта (когда хакер пытается подобрать пароль, программа-робот в первую очередь подбирает пароли, известные ей из базы данных украденных паролей).

5. Версия Вашей CMS (joomla, wordpress и т.д.) всегда должна быть актуальна, следите за обновлениями. Если был найден уязвимый код в структуре сайта, а Вы своевременно не обновились, то Ваш сайт автоматически попадает в зону риска, в этом случае взломщик не подбирает пароли, а пользуется известной уязвимостью старой версии CMS.

6. Храните актуальную и рабочую версию сайта у себя на компьютере или USB-накопителе, раз в месяц копируйте сайт на локальный компьютер (USB-

накопитель). В случае каких-либо неисправностей или подозрений на вирус - рекомендовано удалить последнюю версию сайта и загрузить ту, в которой Вы уверены. Перед восстановлением (загрузкой) рекомендовано сменить пароли (виртуальная панель, ftp:// , административная панель CMS (/administrator, /wp-admin и т.д.)) и проверить обновления на движок сайта (CMS).

7. Следите за содержимым, сайт — это не файловая «помойка». Если Вы нашли лишние папки, файлы, которых раньше не было, и при этом Вы ничего нового не устанавливали, скопируйте папки с актуальной версией сайта себе на компьютер (USB-накопитель), удалите лишние файлы, обновите сайт и просмотрите его функционал. Если всё работает, то, скорее всего, это был вирус. В этом случае рекомендуется вернуться к пункту 6 (обновить CMS, сменить пароли).

Одни из самых слабых мест в CMS – папки, открытые для частого редактирования, такие как images, docs, так как с ними работают и обычные пользователи. Эти папки уязвимы, т.к. в них могут быть добавлены файлы с вредоносным кодом. Для того, чтобы частично себя обезопасить (это не даёт 100% защиты), в эти папки должны быть добавлены файлы **.htaccess** (файл должен называться именно так) со следующим содержанием:

Подходит любая из двух следующих команд:

1-я:

<Files ~ "\.(php|php3|php5|php4|phtml)$">

deny from all

</Files>

2-я:

php_flag engine off

RemoveHandler .phtml .php .php3 .php4 .php5 .php6 .phps .cgi .exe .pl .asp .aspx .shtml .shtm .fcgi .fpl .jsp .htm .html .wml

AddType application/x-httpd-php-source .phtml .php .php3 .php4 .php5 .php6 .phps .cgi .exe .pl .asp .aspx .shtml .shtm

.fcgi .fpl .jsp .htm .html .wml

Обе команды запрещают обрабатывать файлы данных расширений, следовательно, вредоносный код в них тоже работать не будет.

На эти файлы нужно выставить права: **444**

Также вредоносный код может заливаться и в папки /tmp и /logs, сюда же создаём файл **.htaccess (файл редактируется любым текстовым редактором)** и пишем в нём команду:

Deny from all

Права на файл: **400**

Подробную информацию о том, что такое:

- «Права на папку», Вы можете прочитать перейдя по ссылке http://en.wikipedia.org/wiki/Chmod

- «Как правильно выставить права на файлы и папки», Вы можете прочитать перейдя по ссылке http://joomlaforum.ru/index.php/topic,101915.0.html

- «Что делать, если вас всё-таки взломали?»

http://joomlaforum.ru/index.php/topic,246899.0.html

Напоминаю, во избежание лишних вопросов: **Защитой сайта занимается непосредственно Локальный администратор**, т.е. Вы, локальный администратор школы, детского сада и прочих образовательных организаций.

В случае возникновения технических вопросов необходимо обращаться в ТОГБУ «Компьютерный центр» к инженеру-программисту Бавину Дмитрию Владимировичу по электронной почте bavin@68edu.ru или по телефонам 8(4752)53-01-48, 8(4752)47-60-05.

Полезные ссылки:

http://joomlaforum.ru

http://joomlaportal.ru/content/view/68/53/

http://www.joomla.org/

http://ru4ek.net/yunomu-sisodminu/31-opyat-pro-zashchitu-joomla

https://www.google.ru/