ЗАЩИТА ВЕБ-СЕРВЕРОВ, РАБОТАЮЩИХ НА "APACHE"

Криштопин А.В., Губенко Н.Е.
Донецкий национальный технический университет

Независимо от задач, которые призван решать ваш узел, вопросы его безопасности требуют особого внимания. Особенного внимания проблема безопасности требует при создании узла, предназначенного для электронной коммерции. Если вами не будет предпринято существенных мероприятий по укреплению безопасности веб-сервера, то появляется риск утечки конфиденциальной информации. Именно поэтому необходимо уделить пристальное внимание вопросам безопасности. В контексте самого распространенного на сегодняшний день сервера «Apache» проблема безопасности является одной из приоритетных. В докладе будут рассмотрены проблемы безопасности на уровне операционной системы и способы предотвращения нескольких очевидных «дыр» в ее защите. Отдельные части доклада посвящены проведению соответствующего исследования. Также будет рассмотрен метод настройки сервера Apache для обеспечения максимальной безопасности. Этот раздел включает информацию о том, что следует делать для того, чтобы повысить безопасность системы. Затем будет рассмотрена проблема санкционирования доступа пользователей. Существует множество механизмов идентификации пользователей. Одни из них гарантируют доступ на основании анализа источника запросов; другие базируются на схемах идентификации имени пользователя и его пароля. В конце доклада будут обсуждены механизмы обеспечения безопасной передачи данных в Apache с применением протокола SSL (Secure Sockets Layer -протокол защищенных сокетов).

Без достаточно надежной операционной системы нет смысла предпринимать все остальные шаги для защиты сервера. В докладе подробно описываются некоторые основные этапы повышения безопасности работы сервера в операционной системе и настройки сервера Apache. Политика безопасности позволит организовать корректный доступ к информации хранящийся на сервере. Принципы этой политики должны быть четко и ясно сформулированы и опубликованы организацией. Политика должна определять, кому разрешен доступ к вашим компьютерам, когда им разрешается осуществлять этот доступ и что разрешается делать в системе после регистрации.

Еще одним из рекомендуемых действий является ограничение: сервер не должен работать на машине, где производится разработка программного обеспечения. Если на компьютер возложена только задача обработки Web-запросов, все остальные задачи с него нужно убрать. Кроме того, чем меньше людей имеют возможность для регистрации на сервере, тем меньше возможности появления "дыр" в системе безопасности как случайных, так и преднамеренных.

Фактически каждый продавец программного обеспечения как коммерческого, так и некоммерческого, периодически рассылает доработки, произведенные в связи с найденными ошибками и пробелами в системе безопасности. Раз в месяц необходимо посвятить несколько часов для загрузки новых доработок к операционной системе и основным программным пакетам. Обязательно требуется вести дневник обновлений.

Одной из причин нарушения безопасности являются CGI-сценарии. CGI-сценарии и программы уже сами по себе несут опасность, так как они **разрешают**

произвольному пользователю запускать программы в вашей системе. Преднамеренно или нет, каждый новый сценарий может содержать ошибки.

Для корректной работы требуется обучить разработчиков системы и обучиться самому ситуациям, при которых возникают пробелы в системе зашиты. Например, всегда необходимо проверять размер длины строк, вводимых пользователями, для того, чтобы избежать использования злоумышленником ситуации переполнения буфера. Существует множество Web-узлов, которые специализируются исключительно на проблемах безопасности.

Никогда не следует загружать программы из Internet, если нет четкого понимания их функций.

Также следует хранить свои CGI-сценарии и программы в отдельном подкаталоге. Любое другое место кроет в себе возможность оплошности или ошибки. Существует вероятность возникновения такой ситуации, при которой вы не можете четко сказать, где находятся ваши программы, а не то, чтобы позаботиться об их безопасности.

Язык положенный в основу ранних версий PHP допускает возможность переполнения буфера, что позволяло пользователям выполнять на локальном компьютере произвольные программы. Эта проблема была решена только в последних версиях. Таким образом, Достаточно убедиться в том, что на сервере установлена последняя версия PHP.

Вставки на стороне сервера должны быть настроены таким образом, чтобы пользователи не имели возможность запускать на сервере произвольные программы.

Опасность может возникнуть, если пользователи смогут определять собственные права доступа. Кроме того, файлы .htaccess отрицательно влияют на производительность. По этой причине директивы AllowOverrides должны быть установлены в None.

В докладе будут рассмотрены следующие разделы:

- Указания по настройке
- Основы идентификации
- Идентификация пользователей
- Протокол SSL

Литература

[1] http://securitylab.ru/analitics/240126.php (на 05.11.2005)

[2] http://apache.org/manual/security.php (на 15.11.2005)