Защищаем сайты

Виктор Кобзарев,
системный администратор
УП «Надежные программы»

Утечка информации, некорректное функционирование сайта, испорченная репутация… История насчитывает миллионы печальных примеров проникновения на веб-ресурсы. Подбор паролей или расщепление HTTP-запроса — да мало ли какой способ атаки изберет злоумышленник.

Справка ТБ

Виктор Кобзарев. В 2005 году окончил Белорусский государственный университет информатики и радиоэлектроники, специальность — инженер по автоматическому управлению в технических системах. Опыт работы: 2005-2006 гг. — ОАО «Пеленг», инженер по автоматическому управлению; 2006-2009 гг. — Белтелерадиокомпания, ведущий инженер-программист; с 2009 по настоящее время — УП «Надежные программы», системный администратор.

Способов много, а причина уязвимости одна — недостаточная защищенность. Путь к минимизации рисков — защищенный хостинг. Все вы прекрасно знаете, что для функционирования сайта, кроме доменного имени (названия сайта), необходима услуга хостинга. Виртуальный хостинг (shared), VPS (Virtual Private Server), Colocation — каждый заказчик может выбрать приемлемый по цене и производительности вид услуги.

Время от времени веб-ресурсы клиентов подвергаются атакам. Сегодня одним из самых популярных сайтов, предоставляющих информацию о том, какие веб-приложения уже подверглись атаке, является www.stopbadware.org. Сайт бесплатный, его поддерживают такие крупные компании, как Google и Firefox.

Сейчас в базе данных stopbadware находится около миллиона зараженных ссылок, и это число постоянно увеличивается. Именно поэтому клиенты, желающие свести к минимуму нежелательные последствия вторжения злоумышленников, выбирают защищенный хостинг.

Атаки на сайты

Различают следующие виды атак:

1. **Аутентификация**. Данный вид атак направлен на используемые Web-приложением методы проверки идентификатора пользователя, службы или приложения. Аутентификация использует как минимум один из трех механизмов (факторов): «что-то, что мы имеем», «что-то, что мы знаем» или «что-то, что мы есть». Эти атаки направлены на обход или эксплуатацию уязвимостей в механизмах реализации аутентификации Web-серверов.

2. **Авторизация**. Данный вид атак направлен на методы, которые используются Web-сервером для определения, имеет ли пользователь, служба или приложение необходимые для совершения действия разрешения. Многие Web-сайты разрешают доступ к некоторому содержимому или функциям приложения только определенным пользователям. Доступ другим пользователям должен быть ограничен. Используя различные техники, злоумышленник может повысить свои привилегии и получить доступ к защищенным ресурсам.

3. **Атаки на клиентов**. Открыв сайт, вы хотите получить доступ к какому-то сервису или информации. Во время посещения сайта между пользователем и сервером устанавливаются доверительные отношения — как в технологическом, так и в психологическом аспектах. Пользователь ожидает, что сайт предоставит ему легитимное содержимое. Кроме того, пользователь не ожидает атак со стороны сайта. Пользуясь этим доверием, злоумышленник может прибегать к различным методам проведения атак на клиентов сервера.

4. **Выполнение кода**. Этот вид атак направлен на выполнение кода на Web-сервере. Все серверы используют данные, переданные пользователем при обработке запросов. Часто эти данные используются при составлении команд, применяемых для генерации динамического содержимого. Если при разработке не учитываются требования безопасности, злоумышленник получает возможность модифицировать исполняемые команды. Внедрение серверных сценариев — это внедрение какого-либо вредоносного кода, который выполнится на сервере в запущенном веб-приложении. Так как оно запускается с правами и привилегиями полноценного пользователя, вы можете столкнуться с очень большими проблемами.

5. **Разглашение информации**. Данный вид атак подразумевает, что злоумышленник любыми способами будет пытаться получить информацию о ваших сервисах. В частности, это идентификация приложений: мы получаем версию ПО веб-сервера, язык и, соответственно, можем узнать текущие уязвимости сайта. Еще одна из угроз — утечка информации. Например, в Беларуси в комментарии java-скрипта, т.е. кода, который выполняется на стороне клиента, находилась информация о том, как программист писал данный код. Это дополнительная информация и ею можно воспользоваться.

6. **Логические атаки**. Данный вид атак подразумевает следующее: злоумышленник представляет себе логику вашего приложения и будет стараться использовать ее в своих корыстных целях. Самый простой пример — отказ в обслуживании, когда вы нагружаете сервер запросами.

Защищенный хостинг: для кого-то он обязателен?

Этот тип хостинга необходим, прежде всего, государственным органам и организациям, которые используют в своей деятельности сведения, составляющие государственные секреты.

Для решения проблемы конфиденциальности достаточно давно была предложена идея размещения сайтов таким образом, чтобы вероятность атак была минимальной. В 2010 г. ОАЦ при Президенте РБ от слов перешел к конкретным действиям: была создана документация, описывающая требования к защищенному хостингу. Одно из положений Указа № 60, направленного на улучшение работоспособности нашего Интернета в целом, говорит: если вы являетесь государственной организацией и ваша работа связана с использованием государственных секретов, вы обязаны размещать сайт на защищенном хостинге. Таким образом, чтобы минимизировать угрозы безопасности данных, все серьезные организации (банки, крупные коммерческие организации) должны перейти на защищенный хостинг.

Переход на защищенный хостинг

Во-первых, для перехода на защищенный хостинг необходимо определиться с типом размещения. Выделяют три типа размещения: виртуально-защищенный сервер, виртуальный (shared) хостинг и выделенный сервер, который находится на защищенной площадке.

На виртуальном хостинге разрешено размещать только сертифицированные системы управления сайтом. На данный момент их также три:

1. СУС «CMS DEW POWER» (ОАО «Гипросвязь»);
2. SectorCMS 1.4. (РУП «Белтелеком»);
3. Программные средства управления сайтом (разработка Центра информационных ресурсов и коммуникаций БГУ).

Если сайт использует любые другие программные решения (в т.ч. собственной разработки), либо проект имеет повышенные требования к ресурсам сервера — необходимо размещать его исключительно на выделенном сервере.

На данный момент существуют 7 организаций, которые уполномочены представлять услуги защищенного хостинга:

1. Научно-производственное частное унитарное предприятие «Надежные программы».
2. Государственное учреждение «Главное хозяйственное управление» Управления делами Президента Республики Беларусь.
3. Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси».
4. Белорусско-английское совместное предприятие общество с ограниченной ответственностью «Деловая сеть».
5. Республиканское унитарное предприятие электросвязи «Белтелеком».
6. Закрытое акционерное общество «ГЛОБАЛВАНБЕЛ».
7. Общество с ограниченной ответственностью «АйПи ТелКом».

Эти организации полностью прошли процедуру регистрации и включены в реестр ОАЦ при Президенте Республики Беларусь для предоставления такого типа услуг.

Обязанности заказчика:

- Сайт должен принадлежать национальной доменной зоне Республики Беларусь — .by. Исключение составляют 2 зоны, которыми занимается ОАЦ при Президенте Республики Беларусь, — .gov.by и .mil.by (использовать домен в этой зоне можно только с разрешения ОАЦ).
- Сообщить поставщику услуг данные администратора ресурса.

• Сообщить IP-адреса, откуда будет администрироваться ресурс.

• Выбрать протоколы транспортного уровня, по которым будет осуществляться доступ к ресурсу, и сообщить их поставщику услуг.

• Предоставить данные для регистрации ресурса в БелГИЭ.

• Незамедлительно устранять выявленные нарушения безопасности сайта, если хостинг-провайдер не может их устранить собственными силами.

Обязанности поставщика услуг:

• Фильтровать трафик от вредоносного программного обеспечения.

• Обеспечивать бесперебойное электропитание используемого оборудования.

• Размещать сайт заказчика на оборудовании, находящемся на территории Республики Беларусь.

• Осуществлять мониторинг работоспособности Интернет-сайта, серверов, средств защиты информации с постоянным оповещением администратора безопасности о нарушениях функционирования системы защиты информации.

• Незамедлительно устранять выявленные нарушения безопасности Интернет-сайтов. При невозможности их устранения собственными силами в течение одного дня информировать ОАЦ и администраторов соответствующих Интернет-сайтов.

• Применять сертифицированные средства защиты информации.

• Обеспечивать ежедневное обновление используемого для оказания Интернет-услуг программного обеспечения.

• Предоставлять доступ государственным органам и организациям к сетям общего пользования только по портам протоколов транспортного уровня, определенным договором на оказание Интернет-услуг.

• Обеспечивать синхронизацию системного времени на серверном оборудовании от службы единого времени белорусского государственного института метрологии.

Защищенный хостинг: как он работает?

На защищенном хостинге реализована защита от угроз и атак, о которых мы говорили в начале статьи. Она достигается следующими средствами:

• Межсетевое экранирование аппаратными средствами.

• Защита целостности ресурса (дефейс, фишинг, взлом).

• Ограничение административного доступа.

• Анализ поступающих запросов на уровне http-протокола.

• Защита от DDoS-атак.

• Использование оборудования премиум-класса.

• Сертифицированные ОАЦ средства защиты информации.

• Система аудита и протоколирования событий безопасности ресурса.

• Постоянное резервное копирование.

• Круглосуточный мониторинг.

• Защищенная почта (шифрование SSL и ограничение по IP-адресу).

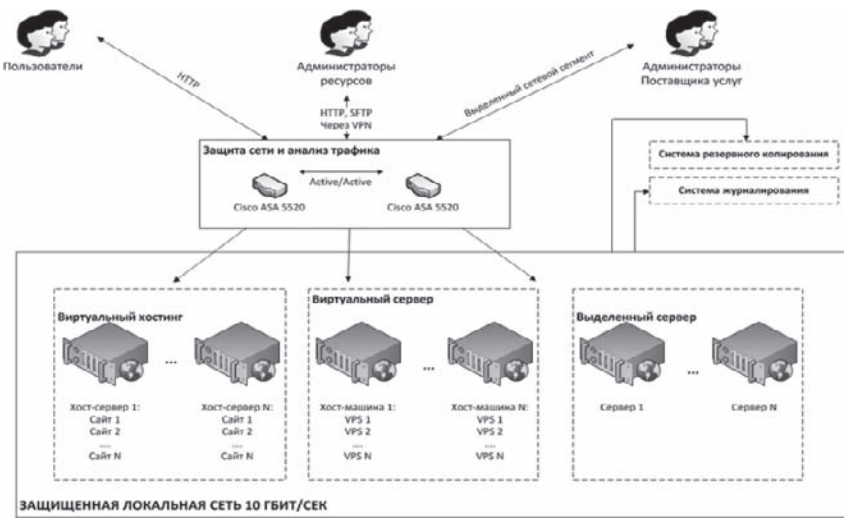
• Тестирование защищенности ресурса (компания BelSoft).

Для предоставления услуг используется оборудование премиум-класса — HP BladeSystems C7000. Это очень качественное аппаратное решение на сегодняшний день.

Фильтрация трафика осуществляется оборудованием Cisco ASA5520. Это оборудование сертифицировано в ОАЦ. Оно осуществляет глубокий анализ поступающего трафика и обнаруживает вредоносный код, защищает от DDoS-атак, обеспечивает функционирование защищенной зоны с доступом по протоколу L2TP over IPSec с поддержкой шифрования AES. Кроме того, происходит полное резервирование оборудования.

Наша компания (hoster.by) предлагает 3 типа услуг защищенного хостинга: виртуально-защищенный сервер, виртуальный (shared) хостинг и выделенный сервер. Существует три типа доступа к серверам, каждый из которых осуществляется по защищенному протоколу для административной части ресурса. Обычные пользователи не видят внутреннюю сеть этих ресурсов, получается, что серверы полностью разграничены логически. Внутри работают серверы, и эта сеть изолирована с помощью Cisco ASA5520 от внешнего мира. У нас есть свой сегмент сети, и мы осуществляем администрирование ресурсов только из него. Администраторы ресурсов имеют доступ к своей административной части только с определенных IP-адресов, поэтому, чтобы взломать такую систему, злоумышленнику необходимо знать IP-адрес владельца ресурса. По-другому не получится.

Наша компания заинтересована в оказании клиентам действительно качественных услуг хостинга. Мы всегда идем навстречу своим пользователям, оказываем помощь в переносе сайта на защищенную площадку при отсутствии у клиента собственных специалистов. ■



УП «Надежные программы» (hoster.by)
220005, г. Минск, ул. В.Хоружей, 1А, 6 этаж
Тел.: +375 17 239-57-02,
velcom: +375 29 3-4444-83,
МТС: +375 29 776-44-83,
life: +375 25 720-52-66,
факс +375 17 239-57-20
info@hoster.by