ния организациями малого бизнеса // Экономика. Налоги. Право. 2015. № 2. С. 94–100.
6. Орлов А. И. О некоторых подходах к экономико-математическому моделированию малого бизнеса // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2015. № 108. С. 288–315.
7. Kalkan A., Bozkurk Ö.C. The choice and use of strategic planning tools and techniques in Turkish SMEs according to attitudes of executives // 9th International Strategic Management Conference. Procedia – Social and Behavioral Sciences. 2013. No. 99. Pp. 1016–1025.
8. Gică O. A., Balint C. I. Planning practices of SMEs in North-Western Region of Romania an empirical investigation // Emerging Markets Queries in Finance and Business. Procedia Economics and Finance. 2012. No. 3. Pp. 896–901.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВЕБ-САЙТОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Пузанков Артем Михайлович
3 курс, факультет «Информационных технологий»
Московский политехнический университет

Чикунов Иван Михайлович
кандидат технических наук, заведующий кафедрой «Инфокогнитивные технологии» Московского политехнического университета

Аннотация: *В данной статье рассматриваются вопросы обеспечения безопасности серверов и веб-сайтов, плюсы и минусы реализации серверов в домашних условиях, а также различные современные технологии защиты серверов и веб-сайтов.*

Ключевые слова: *сервер, веб-сайт, защита, брандмауэр, виртуальная частная сеть, аудит.*

Abstract: *This article discusses the security of servers and websites, the pros and cons of implementing servers at home, as well as various modern tech-nologies to protect servers and websites.*

Keywords: *server, website, security, firewall, virtual private network, audit.*

Введение. В настоящее время информационные технологии начинают играть ключевую роль в постиндустриальной экономике. Следовательно, безопасность веб-сайта и сервера – один из наиболее важных составляющих информационной безопасности. В частности, безопасность и защита сайта – задача, с которой рано или поздно встречается владелец ценного ресурса. Вопрос безопасности можно решить, как на этапе проектирования, так и вернуться к нему в случае возникновения проблем[3].

Согласно данным проекта Web Application Security Statistics Project, в котором было проанализировано более 12000 веб-приложений, более 13% сайтов могут быть взломаны полностью с помощью обычных тестов. Около 49% веб-приложений содержат уязвимости высокого уровня, которые были найдены в ходе автоматического сканирования. Около 80-96% сайтов, которые предоставили исходные коды и были тщательно проанализированы, оказались с серьезными уязвимостями. Статистика показывает, что безопасности нужно уделять большее внимание.

Основная угроза безопасности сайта – хакерская атака. Она может быть либо целевой, либо по принципу «атакую всё подряд», то есть носить бессистемный характер. Основным источником угроз информационной безопасности в веб-приложениях являются внешние нарушители. Внешний нарушитель – лицо, не имеющее доступа к сайту, имеющее высокую квалификацию в вопросах обеспечения сетевой атакой. В первом случае злоумышленник может выявить максимальное количество возможных атак и реализовать наиболее успешные, во втором случае обычно используются несколько поверхностных уязвимостей.

К примеру, сейчас множество государственных услуг оказывается через такие сайты как сайт «Государственные Услуги» (gosuslugi.ru), «Официальный сайт мера Москвы» (mos.ru). Можно обеспечить идеальную защиту на сайте, но забыть про серверы, на которых они расположены.

Рассмотрим виды серверов. На сегодняшний день существуют несколько разновидностей серверов: VDS/VPS, выделенный сервер, сервер, организованный пользователем у себя дома и др.

Ниже приводятся три эффективные способа защиты серверов[1]:

1. Firewall (фаервол или же брандмауэр) – программное или программно-аппаратное обеспечение, которое фильтрует сетевой трафик и контролируют доступ к сети. Это означает блокирование или ограничение доступа к каждому открытому порту, кроме исключений. Тщательно настроенный брандмауэр будет блокировать доступ ко всему, для чего вы сами назначите исключение. Уязвимые для атаки компоненты, прикрытые фаерволом, уменьшат поверхность атаки на сервер.
2. VPN (виртуальная частная сеть) – способ создать защищённое соединение между удалёнными компьютерами и текущим узлом. Даёт возможность настроить свою работу с сервером таким образом, будто используется защищённая локальная сеть. Использование VPN – способ создания частной сети, которую смогут видеть только включенные в нее серверы. Связь будет полностью приватной и безопасной. Так же, VPN можно настроить для отдельных служб и приложений, чтобы их трафик проходил через виртуальный интерфейс[1,2].
3. Аудит файлов и система обнаружения вторжений. Аудит файлов – процесс сравнения состояния текущей системы с записями файлов и характеристиками системы, когда она находится в исправном состоянии. Метод применяется для обнаружения изменений, при которых нужна авторизация. Система обнаружения вторжений – часть программного обеспечения, которая контролирует систему или сеть на несанкционированные действия. Многие хостинговые системы используют аудит файлов как метод проверки на изменения в системе. Аудит файлов — это способ удостовериться в том, что файловая система не изменена кем-либо (пользователем или процессом).

Безопасность сайтов зависит от качества их программного кода и от компетентности администратора веб-сервера. То есть причиной угроз безопасности, может быть, как уязвимость самого сайта перед кибератакой (например, отсутствие защиты от перебора паролей), так и ошибки, допущенные администратором веб-сервера (например, несвоевременное обновление ПО). Не менее частой причиной взломов является незна¬ние или несоблюдение сотрудниками банальных правил безопасности (простые пароли, ввод данных на фишинговых сайтах, заражение вирусами ПК администраторов). Рекомендации для защиты сайта:

- Доверять разработку требовательных к уровню безопасности сервисов опытным специалистам, новички, как правило, могут добиться работоспособности приложения, но не в состоянии учесть риски взлома.
- Администрированием сервера должен на регулярной основе заниматься специалист. Большинство заражений сайтов вирусами происходит из-за того, что серверное ПО никто не обновляет.
- В случаях сомнений в безопасности сайта, заказывать аудит безопасности у независимой компании.
- Использовать защищённые протоколы (пример https).

Выбор между виртуальным сервером, выделенным и домашним зависит от многих критериев: бюджета, задач, которые должен выполнять сервер, уровня стабильности и системных рисков. Множество пользователей организовывают серверы дома для относительно простых задач (таких как запуск веб-служб, поддержание простых сайтов-визиток, запуска голосовых служб, OpenVPN и просто в учебно-познавательных целях) и учитывая дешевеющий рубль становится намного выгоднее содержать домашний сервер. В этом случае все риски пользователь принимает на себя, в том числе и организацию защиты сервера. Пользователь сам должен определить оптимальную схему подключения сервера к домашней сети и реализовать необходимые меры по обеспечению безопасности.

Список литературы

1. Джоел Скембрей, Майк Шема, Йен–Минг Чен, Дэвид Вонг Секреты хакеров / Джоел Скембрей, Майк Шема, Йен–Минг Чен, Дэвид Вонг, 2003г. Вильямс;
2. Майк Шиффман Защита от хакеров / Шиффман Майк, 2002г. Вильямс;
3. Поларков Н.И. «Компьютерные технологии», Ростов-на-Дону, «Феникс», 2002г.