Чикунов И.М.

§3.10. Обеспечение безопасности веб-сайтов в эпоху цифровизации.

Проанализированы наиболее общие способы защиты серверов, которые организации могут использовать для предотвращения атак или их смягчения. Рассмотрена безопасность веб-сервера, так как именно он отвечает за прием и обработку HTTP-запросов от клиентов к веб-сайту. Результатам исследования атак на Web-сайты показали, что работоспособность серверов может быть нарушена даже в результате перегрузки одного или нескольких сервисов. Сделан вывод, что необходимо вкладывать средства в системы защиты наиболее уязвимых мест сети, так как они отвечают за базовые услуги и функционирование миллиардов веб–сайтов по всему миру, в результате превращаясь в хранилище персональных данных посетителей.

Ключевые слова. Обеспечение безопасности, сервер, веб-сайт**,** информационные технологии, экономика**.**

Chikunov I.M.

§3.10. Securing websites in the digital age.

Analyzed the most common ways to protect servers that organizations can use to prevent attacks or mitigate them. The security of a web server is considered, since it is he who is responsible for receiving and processing HTTP requests from clients to a website. The results of the study of attacks on Web-sites showed that the health of servers can be impaired even as a result of overloading one or more services. It was concluded that it is necessary to invest in the protection systems of the most vulnerable points of the network, as they are responsible for the basic services and the operation of billions of web sites around the world, as a result of which they turn into a repository of personal data of visitors.

Keywords: Security, server, website, information technology, economy

В настоящее время информационные технологии начинают играть ключевую роль в постиндустриальной экономике. Следовательно, безопасность веб-сайта и сервера – один из наиболее важных элементов информационной

безопасности. В частности, безопасность и защита сайта – задача, с которой рано или поздно встречается владелец ценного ресурса. Вопрос безопасности можно решить, как и на этапе проектирования, так и вернуться к ней в случае возникновения проблем.

Согласно данным проекта Web Application Security Statistics Project, который проанализировал 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. безопасности и большой опыт в реализации сетевых атак на различные типы информационных систем.

Другими словами – основная угроза безопасности сайта – хакерская атака. 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, то есть иметь конечную цель, либо по принципу «атакую все подряд», то есть носить бессистемный характер. В первом случае злоумышленник может выявить максимально возможное 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 сервера на которых они расположены. Рассмотрим виды серверов. На сегодняшний день существуют несколько разновидностей сервера: VDS/VPS, выделенный сервер, сервер, организованный пользователем у себя дома и др.

Выбор между виртуальным сервером, выделенным и домашним зависит от многих критериев: бюджета, задач, которые должен выполнять сервер, уровня стабильности и системных рисков. Уже появляются люди, которые организуют сервер у себя 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.

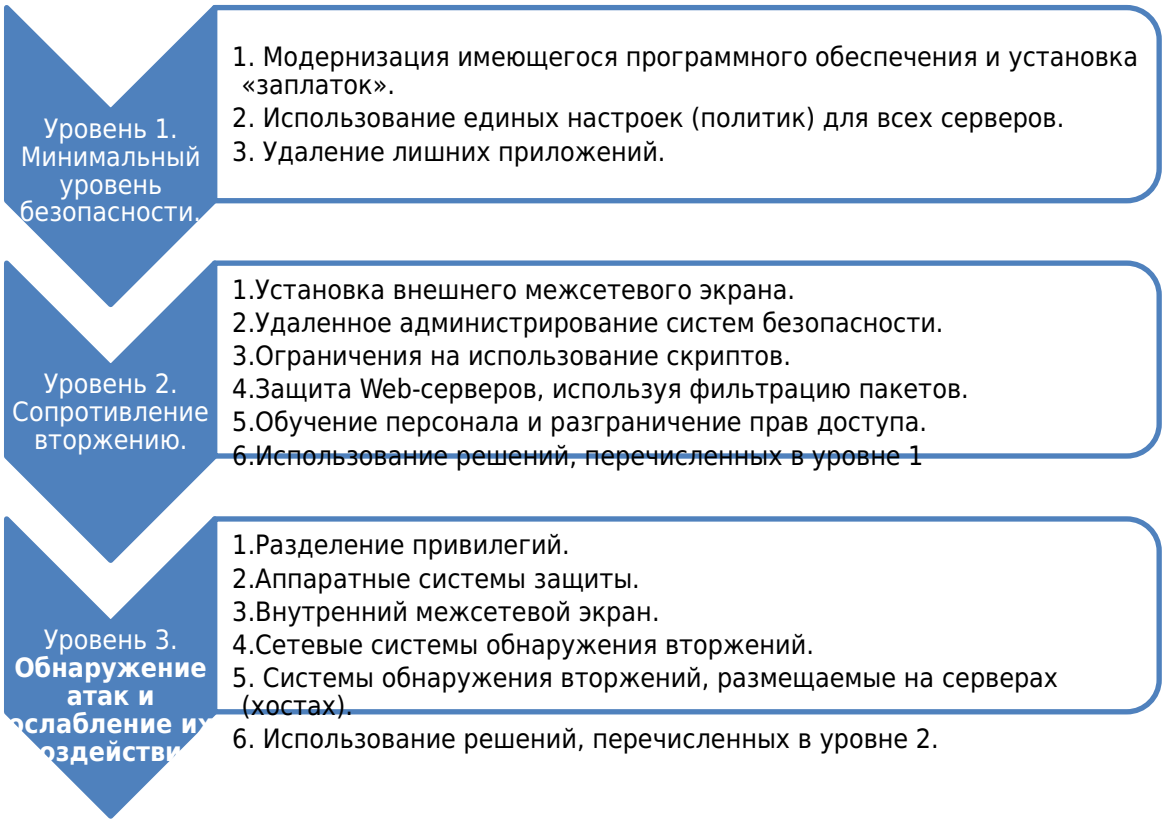

Рисунок 1. Уровни безопасности для сервера

Варианты обеспечение безопасности Web.серверов

Можно выделить следующие, наиболее общие способы защиты Web-серверов, которые представлены на рисунке 2

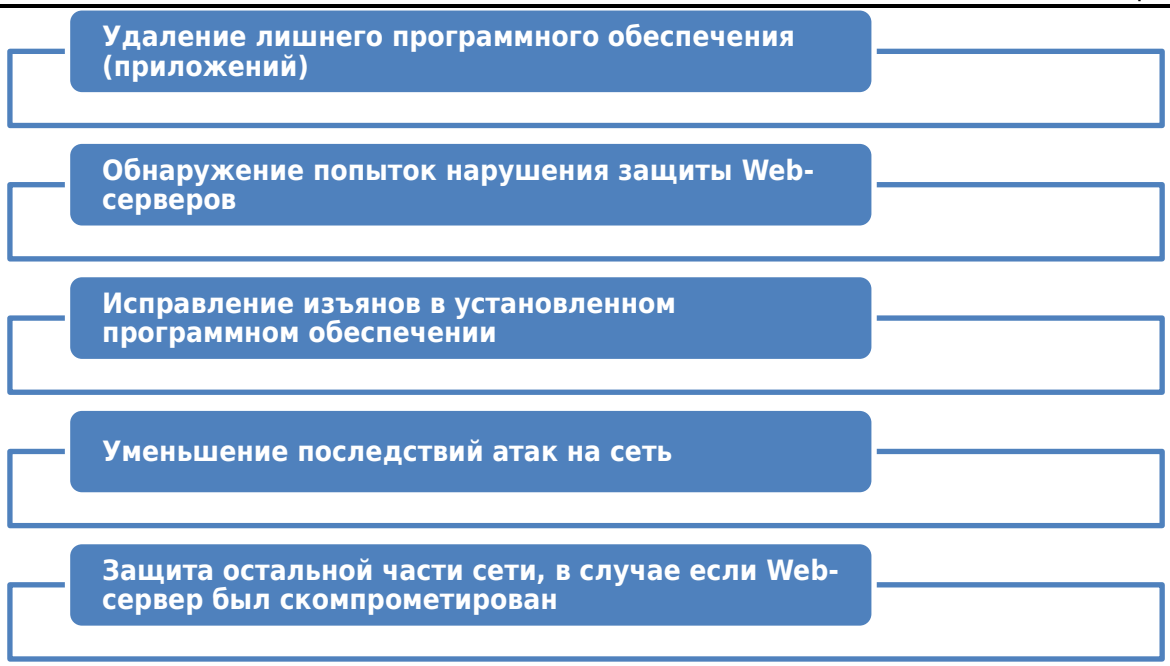

Рисунок 2. способы защиты Web-серверов

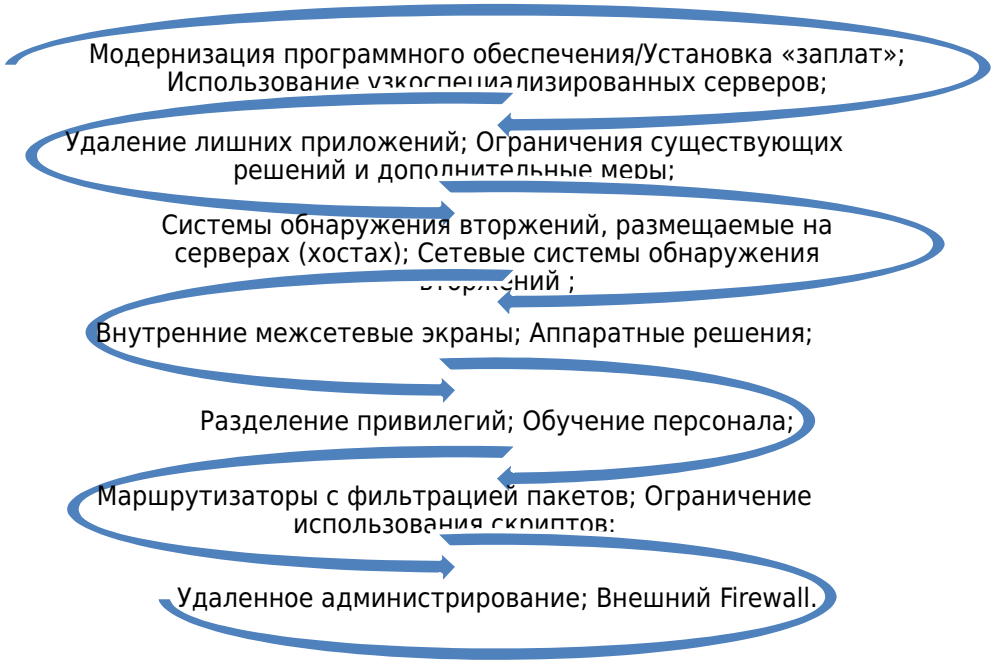

Рисунок 3. Модернизация программного обеспечения

Модернизация программного обеспечения/Установка «заплат»(Рис.3)

Это один из наиболее простых, но вместе с тем наиболее эффективных способов уменьшения рисков. Все имеющиеся Web-серверы должны постоянно (иногда ежедневно) проверяться на предмет обновления установленного

программного обеспечения и установления «заплат». (NIST совместно с другими правительственными организациями разрабатывает специальный инструментарий, предназначенный для оценки необходимости обновления ПО и применения «заплат». Подробности можно найти на страничке Департамента компьютерной безопасности NIST по адресу http: //csrc. nist. gov.)

Требование обновления программного обеспечения вызвано тем, что любое программное обеспечение, установленное на Webсервере, может быть использовано хакером для проникновения в систему. Это операционные системы, программное обеспечение, работающее с сетевыми пакетами или используемое администраторами сети и системы безопасности.

Проверка программного обеспечения должна производиться по следующему алгоритму:

составьте перечень программного обеспечения с указанием номеров версий;

- убедитесь в том, что на вашем сервере установлены последние версии программных продуктов;
- найдите и установите «заплаты» для соответствующих версий программного обеспечения, с учетом прилагающейся поставщиком инструкции. Причем для обеспечения работоспособности системы «заплаты» должны быть установлены в порядке возрастания их номера;
- проверьте, что «заплаты» работают нормально.

Использование узкоспециализированных серверов: Обеспечение безопасности информации требует выделения отдельного ресурса (компьютер) под каждую задачу. В противном случае ошибка в системе безопасности может нарушить работу сразу нескольких сервисов. Например, не желательно размещать сервер электронной почты, Web-сервер и сервер баз данных на одном и том же компьютере. Однако каждый новый сервер должен быть оснащен системой защиты, иначе он может стать легкой мишенью для хакера.

Удаление лишних приложений: Все привилегированное программное обеспечение, не обязательное для Web-сервера, должно быть удалено. Под привилегированным программным обеспечением в данном случае понимается ПО, работающее с сетевыми пакетами или запускающееся с правами администратора. Некоторые операционные системы запускают привилегированные программы по умолчанию, а администраторы часто просто не знают об их существовании. Между тем, каждая такая программа может быть использована хакером для атаки на Web-сервер. В ряде случаев для повышения уровня безопасности администраторы удаляют все программное обеспечение (а не только привилегированное), которое не используется для обеспечения работоспособности Web-сервера.

Внешний Firewall: Установка межсетевого экрана между корпоративной (внутренней) сетью и Web-серверами общего доступа позволяет предотвратить проникновение «левых» пакетов в сеть организации: если злоумышленник проникает на внешний Web-сервер, то попасть в корпоративную сеть организации через firewall ему будет затруднительно. Если же Web-сервер находится внутри корпоративной сети, то хакер, проникнув на него, может, используя захваченный ресурс в качестве плацдарма, нарушить работоспособность всей сети и получить полный контроль над ней.

Удаленное администрирование: Поскольку управлять сервером с физической консоли зачастую не слишком удобно, системные администраторы устанавливают на Web-серверы программное обеспечение, позволяющее осуществлять удаленное администрирование. С точки зрения обеспечения безопасности подобная практика может привести к серьезным проблемам.

В тех случаях, когда удаленное администрирование неизбежно, его необходимо сопровождать следующими действиями:

- шифровать трафик удаленного администрирования (чтобы злоумышленник не смог перехватить управление трафиком сети, получить пароли или внедрить «вредные» команды);

- использовать фильтрацию пакетов (см. описание ниже) при удаленном администрировании из предназначенной для этого конфигурации хоста;
- поддерживать для этой конфигурации более высокий уровень безопасности;
- не использовать фильтрацию пакетов вместо шифрования, так как хакеры могут сфабриковать IP-адреса (посылать сообщения, маскируя свой IP-адрес другим значением).

Ограничение использования скриптов: Большинство сайтов содержат скрипты (маленькие программы), которые запускаются при переходе на особую страницу. Хакер может использовать эти скрипты (при помощи обнаруженных изъянов в коде) для проникновения на сайт. Для обнаружения таких дыр ему вовсе не обязательно знать исходный код, поэтому скрипты необходимо тщательно проверить, прежде чем они будут выложены на сайт. Скрипты не должны запускать случайные команды или посторонние (опасные) программы, позволять пользователям выполнение определенных узкоспециализированных задач, а также ограничивать количество параметров входящего потока. Последнее необходимо для предотвращения атак на переполнение буфера. (При атаках такого рода злоумышленник пытается принудить систему к запуску программы арбитража с целью получения дополнительной информации.) Наконец, скрипты не должны обладать правами администратора.

Маршрутизаторы с фильтрацией пакетов: Маршрутизаторы устанавливают для того, чтобы отделить Webсерверы от остальной части сети. Этот шаг поможет предотвратить многие атаки, не допуская проникновения «чужих» (не правильных) пакетов. Обычно маршрутизаторы удаляют все пакеты, которые не идут на Web-сервер (например, на порт 80) или к портам, использующимся при удаленном администрировании.

Для повышения степени безопасности можно составить перечень пакетов,

подлежащих пропуску. Таким образом, хакеру останется еще меньше возможностей для проникновения в сеть.

Маршрутизатор с функцией фильтрации пакетов будет более эффективен для предотвращения атак при условии удаления с сервера всего ненужного программного обеспечения (злоумышленник не сможет запросить нестандартный сервис). Однако следует иметь в виду, что применение пакетной фильтрации снижает пропускную способность маршрутизатора и увеличивает риск потери «правильных» пакетов.

Обучение персонала: Часто хакеры проникают в систему из-за того, что администраторы сети не владеют знаниями в области обеспечения безопасности или пренебрегают вопросами защиты. Поэтому занимающим эту должность сотрудникам следует постоянно совершенствоваться, изучая системы безопасности сети и используя полученные знания на практике. Несколько отличных книг и учебных семинаров также помогут вашим администраторам.

Разделение привилегий: Независимо от серьезности мер, предпринятых для обеспечения безопасности Web-сервера, вероятность проникновения тем не менее полностью исключить нельзя. Что ж, если это все-таки произошло, важно минимизировать последствия атаки.

Разделение привилегий являет собой эффективный способ для достижения этой цели: каждый пользователь может запускать только определенные программы. Поэтому хакер, проникнувший в сеть по скомпрометированным данным отдельного пользователя, сможет нанести системе лишь ограниченный вред. Например, у пользователя на сайте есть свои страницы, но другие страницы ему недоступны. Следовательно, хакер, добыв данные первого пользователя, окажется не в состоянии как-либо повлиять на прочие ресурсы (страницы). Так же обстоят дела и с программным обеспечением. В целях повышения уровня безопасности для пользователей, обладающих правами записи, можно создать личные поддиректории.

Аппаратные решения: Аппаратура, в плане разделения привилегий, имеет более высокий уровень безопасности, так как в отличие от программного обеспечения не так легко модифицируется. Но через дыры в программном обеспечении хакер может получить доступ и к аппаратным средствам. Одним из наиболее доступных способов защиты от этой угрозы является запрет режима записи на внешние жесткие диски, магнитооптические диски и т. д. Обычно для предотвращения атак Web-сервер конфигурируют на режим «только чтение».

Внутренние межсетевые экраны: Современные Web-серверы часто работают с распределенными системами, они могут взаимодействовать с другими хостами, получать или передавать данные. В этом случае существует большой соблазн разместить эти компьютеры за межсетевым экраном внутри сети организации, обеспечив тем самым безопасность хранимых на них данных. Однако если злоумышленнику удастся скомпрометировать Web-сервер, он может быть использован в качестве стартовой площадки для атаки на эти системы. Для исключения такой ситуации необходимо отделить системы, общающиеся с Web-сервером, от остальной сети внутренним межсетевым экраном. Тогда проникновение на Web-сервер и оттуда на общающиеся с ним системы не приведет к компрометации всей корпоративной сети.

Сетевые системы обнаружения вторжений: Несмотря на все попытки установить «заплатки» на Web-сервер и реализовать безопасную конфигурацию, невозможно добиться гарантированного исключения всех уязвимостей. Тем более что Web-сервер, защищенный от внешних атак, может быть выведен из строя нарушением работы одного из сервисов. В этом случае важно получать оперативную информацию о подобных происшествиях, для минимизации последствий атаки или быстрого восстановления работоспособности сервиса. Для получения такой информации используют сетевые средства обнаружения вторжений.

Сетевые системы обнаружения вторжений (IDS) сканируют весь трафик

сети и выявляют несанкционированную активность, нарушение защиты или блокирование сервера. Современные IDS создают отчет обо всех выявленных нарушениях, одновременно уведомляя о них администраторов путем вывода сообщений на пейджер, электронный почтовый ящик или монитор. Типовые автоматизированные отчеты включают в себя также сбои сетевых соединений и список блокированных IP-адресов.

Системы обнаружения вторжений, размещаемые на серверах (хостах): Системы обнаружения вторжений, размещаемые на серверах, лучше справляются с задачей определения состояния сети, чем сетевые IDS. Обладая всеми возможностями сетевых IDS, во многих случаях серверные IDS лучше выявляют попытки нарушения защиты, так как обладают более высоким уровнем доступа к состоянию Web-сервера.

Однако и этот способ не лишен своих недостатков. Если хакер проникнет на Web-сервер, он сможет отключить серверные IDS, блокировав тем самым получение сообщений об атаке администратором. Удаленные атаки на отказ сервиса (DoS атаки) также часто блокируют IDS на время выхода из строя сервера. А так как DoS-атаки позволяют злоумышленникам блокировать сервер без проникновения на него, то IDS, расположенный на сервере, должен быть дополнен сетевой системой обнаружения вторжений.

Ограничения существующих решений и дополнительные меры: Все специалисты по безопасности советуют использовать защищенное программное обеспечение, но в некоторых случаях установить его невозможно из-за дороговизны или нехватки времени. Мало того, безопасное программное обеспечение через некоторое время устаревает, и необходимо устанавливать новую версию. Поэтому использование устаревшего ПО и стандартных методов обеспечения безопасности не может служить гарантией защищенности серверов. Но устойчивость Webсервера к атакам может быть достигнута при условии использования сформулированных решений обеспечения безопасности совместно с надежным программным обеспечением, под которым, в данном

случае, мы понимаем некоторое программное обеспечение, обладающее определенным уровнем безопасности.

Вывод. Уровень безопасности программного обеспечения, может быть оценен, во-первых, путем анализа ранее совершенных атак на серверы, на которых было установлено такое же (или подобное) ПО. Количество атак показывает насколько устойчиво к ним ПО. Причем надежность программного обеспечения прямо зависит от его качества. Некачественное программное обеспечение не учитывает всех требований к системе безопасности и уже поэтому не надежно.

Во-вторых, некоторые компании, специализирующиеся на создании систем безопасности склонны преувеличивать возможности своих продуктов (в плане отсутствия уязвимостей), поэтому при проектировании систем безопасности своих серверов пользователи должны учитывать это обстоятельство.

В-третьих, оценить уровень безопасности программного обеспечения можно путем тестирования его на наличие уязвимостей.

Существует множество компаний аудиторов, занимающихся проверкой защищенности серверов. Эти компании имеют в своем арсенале специализированное программное обеспечение, позволяющее выявлять дыры в системах безопасности.

Библиографический список

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. Полярков Н.И. «Компьютерные технологии», Ростов-на-Дону, «Феникс», 2002г.