Угрозы безопасности Web-порталов и методы защиты

Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*
Роман Ванерке, *руководитель отдела технических решений АО "ДиалогНаука"*

На сегодняшний день Web-портал компании, доступный в сети Интернет 24 часа 7 дней в неделю, может выступать в качестве одного из первых объектов, с которого злоумышленники начинают вторжение в корпоративную сеть, поэтому именно здесь должен быть расположен и первый бастион для защиты от возможных атак. Рассмотрим основные типы угроз безопасности Web-порталов, а также те инструменты, которые позволяют значительно снизить вероятность успешной атаки.

DDoS-атаки

Очень часто Web-портал является инструментом для ведения бизнеса, остановка которого может привести к недополученной прибыли и прямым финансовым потерям. Это особенно характерно для банков, предприятий интернет-торговли, платежных систем и др. Хакеры знают о важности Web-порталов для коммерческих и государственных организаций и регулярно проводят взломы с помощью распределенных DDoS-атак, целью которых является нарушение работоспособности портала. Такие атаки могут осуществлять как вымогатели, которые требуют заплатить за прекращение атаки, так и конкуренты, пытающиеся затормозить развитие бизнеса компании. Как правило, современные DDoS-атаки организуются с помощью сети зараженных вредоносной программой компьютеров – бот-сети, ресурсы которой используются для нападения на портал. Цель атаки – исчерпать ресурсы входного канала связи, по которому подключен Web-портал, чтобы легитимные пользователи не могли получить доступ к соответствующим информационным ресурсам. Необходимо отметить, что DDoS-атаки часто используются для отвлечения внимания от основной атаки, которая осуществляется на компанию.

Защититься от такого нападения можно с помощью фильтрации постороннего трафика, который используется злоумышленниками для загрузки каналов связи. Для этого на рынке информационной безопасности представлены специализированные продукты, которые устанавливаются на стороне заказчика и выполняют функции фильтрации трафика. Примерами таких решений являются продукты компаний Arbor Networks, Radware и "МФИ Софт". Некоторый функционал защиты от DDoS также есть в решениях класса WAF (Web-Application Firewall). Кроме этого, существует возможность воспользоваться сервисами по фильтрации трафика, которые предполагают перенаправление входящего трафика на площадку компании, которая займется очисткой трафика, после чего он уже передается заказчику. Подобные услуги предлагают компании Qrator, "Лаборатория Касперского" и наиболее крупные операторы связи.

Атаки на Web-приложения

Web-приложения традиционно базируются на одном из сценарных языков: PHP, Python, Ruby и других, которые являются интерпретируемыми. У злоумышленника есть возможность с помощью специальных символов встроить свой код в запрос к серверу (например, в поисковой строке или в любой другой строке, которая подразумевает ввод данных пользователем) и заставить интерпретатор выполнить посторонний сценарий. Такой метод атаки называется "инъекция" (например, PHP-инъекция, если встраиваются команды для интерпретатора PHP). Поскольку большинство Web-порталов базируется на СУБД с поддержкой интерпретируемого языка SQL, то и команды этого языка также можно навязать к исполнению. Такую атаку называют SQL-инъекцией – она позволяет манипулировать данными в базе, например, связанными с аутентификацией пользователей.

Защититься от большинства видов атак на Web-приложения можно с помощью фильтрации входного потока данных, т.е. HTTP-запросов пользователей и его профилировании (система сперва обучается и далее начинает понимать, какие типы данных ожидать на вход, а также их длину и другие параметры). Для этого, например, можно использовать так называемые экраны Web-приложений WAF. В частности, решения подобного класса предлагают компании Positive Technologies, Imperva, F5 и др. Кроме этого, исходный код Web-приложения при его добавлении на Web-сервер целесообразно проверять специальным сканером кода, который позволяет обнаружить наиболее часто встречающиеся ошибки, допущенные на этапе разработки приложения, и выдать рекомендации по их устранению. Такие сканеры могут быть как бесплатными, так и коммерческими – в качестве примера можно привести сканеры MicroFocus Fortify, Infowatch AppercCut и Solar InCode.

Атаки на ПО Web-портала

Web-приложение в некоторых случаях позволяет обратиться напрямую к операционной системе, на которой работает Web-сервер, и выполнить команды от его имени. Для этого используются более сложные атаки на переполнение буфера или другие манипуляции с памятью серверов. Так могут быть атакованы и база данных, и ПО Web-сервера, и любая другая компонента многоуровневого Web-портала.

В качестве средств защиты от таких атак, помимо вышеперечисленных решений, рекомендуется использовать сетевой сканер безопасности, который тестирует все Web-приложение целиком на наличие известных уязвимостей во всех компонентах. Такие сканеры можно использовать либо для аудита текущей конфигурации Web-портала с помощью анализа конфигурационных файлов, либо для имитации внешних сетевых атак и выявления таким образом имеющихся уязвимостей. В качестве примера сетевых сканеров можно привести решения Maxpatrol, Qualys и Nessus.

Заключение

Успешные атаки злоумышленников на Web-портал компании могут нанести прямой финансовый и репутационный ущерб, а также использоваться в качестве плацдарма для вторжения в корпоративную сеть предприятия. Именно поэтому вопросы защиты Web-портала должны быть обязательно отражены в общей стратегии обеспечения информационной безопасности. Кроме этого, средства защиты портала, некоторые из которых были рассмотрены в данной статье, должны обязательно интегрироваться с другими системами защиты, применяемыми в корпоративной сети. Такой подход позволит обеспечить более высокий уровень информационной безопасности компании в целом. ●

NM ●
АДРЕСА И ТЕЛЕФОНЫ АО "ДИАЛОГНАУКА" см. стр. 48