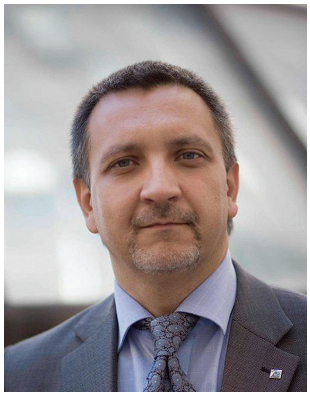
Защита от уязвимостей при доработках web-приложений

В июне 2016 г. ГК Infowatch анонсировала в составе своих партнерских решений нового класса статично-динамическую защиту от уязвимостей при проведении доработок web-приложений, которая позволяет довести время тестирования программных нововведений на наличие "прорех" практически к нулю.



Рустэм Хайретдинов – заместитель генерального директора ГК InfoWatch.

Процесс тестирования вчера и сегодня

Сегодня всё сильнее развивается конфликт между требованиями бизнеса к информационным системам и требованиями информационной безопасности.

Бизнес постоянно ускоряется – требует более быстрых изменений бизнес-приложений, гибкости процессов, скорости разработки новых функций. Конкуренция заставляет компании сокращать время вывода новых сервисов (time-to-market) и переходить на модульную гибкую разработку процессов и приложений (agile).

Процессы исследования же приложений не менялись годами – и самый критичный из них – это процесс взаимодействия исследователей защищённости и разработчиков. Традиционный, сложившийся годами подход: программисты заканчивают разработку бизнес-приложения или его модуля, затем передают исследователям на анализ, те возвращают отчёт с замечаниями, программисты исправляют эти замечания или мотивированно отказываются от исправлений; приложение снова исследуется – и так, возможно, несколько раз. Если компромисса с программистами о закрытии всех уязвимостей достичь не удаётся, то отчёт о найденных уязвимостях отдаётся бизнес-заказчику, который принимает решение: что важнее – быстрый запуск уязвимого приложения или закрытие уязвимостей.

Такой процесс исследования защищённости может занимать месяцы, и это устраивало бизнес до тех пор, пока time-to-market исчислялось полугодиями или годами. Но сегодня бизнес требует выведения новых функций ежемесячно, еженедельно, ежедневно и даже ежечасно и это не преувеличение. Напомним, что Герман Греф, Председатель Правления Сбербанка, на Гайдаровском форуме в феврале 2016 года приводил пример американской компании "Амазон", которая проводит в своих системах изменения до десяти тысяч раз в день, а каждое изменение системы – это потенциальная уязвимость. Изменения в системе не обязательно означают изменение в коде или функционале приложения – на деле функционал даже на самых крупных порталах меняется несколько раз в день, остальные изменения – это изменение настроек, добавление новых пользователей или документов в хранилище и т.п. А значит, безопасности надо учиться быть быстрой, чтобы не стать самым медленным процессом на пути от идеи до функции.

Подходы к тестированию

Есть несколько способов ускорить этот процесс. *Первый* – начать этап исследования уязвимостей ещё на стадии разработки, чтобы к моменту ее окончания уже иметь полный перечень гипотез об уязвимостях, для этого обычно используют статический анализ исходных кодов программ, что позволяет исследовать приложение, не дожидаясь полной сборки. Тогда после окончания разработки исследователям можно будет сразу начать работать над проверкой уже конкретных гипотез, что драматически сокращает время исследования.

Второй способ ускорить процесс исследования – одновременно с выдачей замечаний программистам выпускать «виртуальные патчи»: набор правил для блокирования команд к приложению, если эти команды представляют собой «эксплойт» – последовательность команд, эксплуатирующих уязвимость.

Такой подход позволяет безопасно выпускать в промышленную эксплуатацию бизнес-приложения с уязвимостями.

Как можно тестировать уже сегодня

Для веб-приложений уже сегодня есть приложения полного цикла, позволяющие осуществлять исследование функционала «на лету» – статический анализ (SAST – static application security testing) генерирует гипотезы об уязвимостях ещё на стадии разработки. Динамический анализатор (DAST – dynamic application security testing) исследует эти гипотезы, выпуская подтверждающие эксплойты, которые затем блокируются активными средствами защиты – межсетевыми экранами прикладного уровня (WAF – web application firewall) и системами защиты от DDoS-атак. Такие интегрированные системы позволяют принципиально сократить время выведения на рынок новых бизнес-приложений, а также полностью исключить человеческий фактор в процессе исследования приложений на этапе тестирования и их защиты на этапе промышленной эксплуатации.

Эффект такого подхода трудно переоценить, а при полном переходе на методологию agile без него просто нельзя обойтись. Сегодня такую интеграцию разных систем анализа защищённости проводят интеграторы, однако подобные внедрения довольно долговременны из-за отсутствия стандартов обмена информации между приложениями информационной безопасности. Некоторые компании выпускают частичную автоматизацию процесса: WAF+antiDDoS, SAST+DAST, DAST+WAF и т.п. Проект "Атак Киллер" компании "Инфовотч", впервые объединяющий в себе все необходимые компоненты для полностью автоматической активной защиты (статический сканер, динамический сканер, WAF и анти-DDoS), сегодня защищает критичные информационные системы в разных отраслях – государственные услуги, сайты электронной коммерции, интернет-банк и закупочные торговые площадки крупных промышленных компаний. Процесс полностью автоматизирован и уже поддерживает десятки изменений в приложении в день без включения режима самообучения.

Интеграция пассивных средств анализа защищённости (сканеров) с активными средствами защиты – перспективное направление в информационной безопасности. Она позволяет примирить различные интересы участников процесса защиты приложений: функционального бизнес-заказчика, разработчиков, службу информационной безопасности и службу эксплуатации ИТ, ускоряя выпуск бизнес-приложений и высвобождая дополнительные ресурсы для развития информационной системы.

Рустэм Хайретдинов,
ГК InfoWatch.