ЗАЩИТА БЕЗ ГРАНИЦЫ

АКИНИН А. Н.
Генеральный директор компании WEB CONTROL

Активное изменение IT-ландшафта самым серьезным образом влияет на все аспекты информационной безопасности финансовой (и не только) сферы. Вечный поединок щита и меча переходит в новую фазу – фазу скрытых атак и защиты по всем направлениям. Все уходит в «облака», а это значит, что привычного периметра больше нет, а при отсутствии устоявшейся границы – размываются четкие рубежи обороны.

Поэтому вопрос к специалистам информационной безопасности, по большому счету, сводится уже не к тому, чтобы предотвратить реализацию новых угроз, а к тому – что надо сделать, чтобы сохранить безопасность хотя бы на том уровне, который был до появления новых IT-технологий.

К сожалению, сейчас факт взлома и компрометация чего-то (программы, продукта, приложения) не является большой новостью. Не нужно боятся того, что вас взломают. Вас уже взломали, просто вы еще об этом или не знаете, или не понесли потерь: просто потому, что пока еще не стали персонально интересны злоумышленникам. То есть в сфере интереса специалистов не сама проблема взлома, а снижение, а еще лучше предотвращение ущерба от компрометации информационной системы.

Наши гости – заместитель председателя ЦБ РФ Д. Скобелкин и заместитель начальника ГУБиЗИ ЦБ РФ А. Сычев

Нам нужно не импортозамещение, а экспортопригодность.

На Уральском форуме по безопасности финансовых организаций, в котором мы принимаем участие уже не первый год, очень активно шел разговор о технологиях противодействия кибер-угрозам. Мы уже давно не говорим о кибер-безопасности – речь идет о киберустойчивости – а это большая разница. По сути дела, речь идет о возможности и способности информационных систем существовать в условиях «боевых действий», в условиях непрерывной кибер-атаки, которая осуществляется с разных направлений, с разной степенью интенсивности, адресности и глубины проникновения. Речь идет уже не столько о защите от непосредственного кибер-преступника, а о том, как предотвратить ущерб от его действий.

Свои и наши

Не хочу критиковать людей, стоящих вне профессиональной IT-сферы: они почему-то убеждены, что многочисленные угрозы и риски генерируются самим фактом применения, использования в ПО импортных технологий или продуктов. Как следствие – в нашу сферу вносится лозунг всеобъемлющего импортозамещения, перехода на «суверенные» российские разработки.

Убежден, что импортозамещение – это не самоцель. Сейчас в сфере IT-технологий и непосредственно в секторе финтех-компаний практически исчезло понятие «страна происхождения». В нашей отрасли правильно говорить «страна реализации». Практически все продукты сейчас интернациональны, поэтому нет смысла ставить принципиальную задачу вытеснить с российского рынка тот или иной продукт, ту или иную разработку. Если продукт вышел за пределы своей «страны происхождения» и продвигается на внешние рынки, значит, он того достоин, он располагает рядом конкурентных преимуществ и уже в силу этого – потенциально интересен и востребован.

Так что говорить следует не о запрете проникновения к нам иностранных разработок – надо исходить от обратного. Надо стараться, чтобы за пределы нашей страны, на зарубежные IT-рынки столь же успешно выходили отечественные разработки. Если формулировать кратко – нам нужно не импортозамещение, а экспортопригодность. В глобальном мире невозможно насильно заменить хороший товар – плохим.

Уверяю вас – за последние годы такие продукты в России появились, они могут и уже успешно конкурируют с западными разработками. И напрасно кто-то думает, что их, этих продуктов, мало – по пальцам, как говорится, уже не пересчитать. Но дело даже не в количестве. Я, как глава дистрибьюторской компании, нахожусь в постоянном поиске новых решений, новых разработок и вижу, что зрелость отечественных продуктов уже очень высокая. Причем они пригодны уже не только для прямых, точечных продаж, а для выхода на рынок дистрибьюции. Сейчас наша компания работает с производителями продуктов и решений «верхнего десятка», но российские, образно говоря, уже на подходе.

На Уральский форум мы привезли новое интересное решение компании White Source Software- систему анализа открытых исходных кодов. Проще говоря – кирпичиков, из которых и создается затем та или иная программа. Основная идея продукта – контроль opensource-компонентов на всех этапах разработки, начиная с поиска их в публичных репозиториях. Входной контроль очень важен – ведь иной раз просто неизвестно, что и как заключено в исходных элементах будущей программы. Представленный нами продукт очень интересный, о нем подробнее расскажу в основной части статьи, причем вовсе не ради рекламы. В данном контексте он интересен читателям как реальный пример интеграции усилий специалистов самой широкой «географии».

Сошлюсь на еще один пример – наших партнеров из Израиля. Кстати, тут снова весьма неоднозначный вопрос «страны происхождения» – компания израильская, но добрая половина спецов там говорит и думает по-русски… Теперь к делу. Они сейчас выводят на внешний рынок свои инновационные разработки, и при этом одной из первоочередных стран для продвижения избрана Россия. По той простой причине, что наша страна является одной из крупнейших в мире, повторяю еще раз – крупнейших в мире «поставщиком разработчиков»!

Прошу извинить, если звучит как реклама, но данный продукт помогает создавать отечественные программные продукты быстрее и надежнее, то есть работает на импортозамещение.

Программировать – умеем, теперь надо научиться это продавать.

Неоспоримый факт: именно наши специалисты, наши мозги не имеют себе равных. Но проблема не в том, как создать продукт, тут с нами врядли кто-то сравнится. Проблема в правильном позиционировании продукта – как «упаковать» и представить продукт, как его правильно сформировать под потребности потенциального заказчика. Программировать – умеем, теперь надо научиться понимать, что нужно заказчику и как это продавать. Нужно учиться конкурировать с сильными, интересными игроками этого очень сложного рынка информационной безопасности. При этом напомню простую истину, которую гениально сформулировал отец «сингапурского чуда» Ли Куан Ю – «В бизнесе побеждает не сильный, а быстрый!». Не надо бояться «монстров» рынка информационного обеспечения. Монстры неповоротливы просто в силу своих масштабов, а прорывные технологии, инновационные продукты и решения создают именно те, кто быстр и смел.

White Source: проверить «кирпичики»

Теперь позволю себе перейти к конкретному изложению варианта решения одной из тех проблем, которые обозначил выше. Сегодня не только представитель финтех-волны, но и непосредственно банки включились в разработку собственного программного обеспечения. Это вполне понятно – современные банковские «надстройки» не могут создаваться с полного нуля, они используют уже созданные ранее программы или их компоненты. Вполне логично, что процесс разработки стараются максимально упростить и удешевить – и в этом скрывается один из серьезных рисков…

Снизить стоимость и ускорить процесс разработки ПО можно путем применения открытого исходного кода (opensource). Однако, opensource-компоненты также являются и источником рисков: уязвимости могут активно использоваться киберпреступниками, а лицензионные соглашения могут содержать неприемлемые условия для компании-разработчика. Таким образом, компоненты с открытым исходным кодом необходимо тщательно выбирать, а это достаточно трудоемкий процесс, требующий автоматизации.

Зачастую нет смысла писать код «с нуля», если его уже кто-то написал, опубликовал и разрешил использовать в своих проектах. Важно понимать, что если код уже протестирован и опробован сообществом, не значит, что он не содержит критичных уязвимостей. Более того, компоненты с открытым исходным кодом имеют множество типов лицензий. Условия многих лицензий довольно строгие, например, конечные пользователи от вас могут потребовать бесплатно предоставлять исходный код своей разработки, даже если ваш программный продукт платный.

Уральский форум-2018: у стенда WEB CONTROL

С ростом популярности использования opensource при разработке ПО[1], практически у всех разработчиков теперь есть потребность в автоматизации процесса выбора качественных компонентов с открытым исходным кодом. Вручную собирать информацию о безопасности и качеству по каждому компоненту очень трудоемко.

Давайте сделаем краткий исторический обзор. В 2002 году Black Duck Software представил новинку Protex для идентификации открытого исходного кода в программных разработках. В основе был сканер кода, который выявлял фрагменты исходного кода (codesnippets), совпадающие с opensource. Этот метод анализа имел много ложных срабатываний (фрагменты самописного кода идентифицировались как фрагменты открытого кода), а корректировка результатов производилась в ручном режиме. Несколько позже свои решения для сканирования кода предложили и другие компании, наиболее известные из которых – Protecode (сейчас являются частью Synopsys), Palamida (приобретена компанией Flexera Software) и OpenLogic (приобретена компанией RogueWave).

1 По статистическим данным всемирно известного аналитического агентства Gartner (*Gartner User Survey Analysis: Open-Source Software, 2015), уже в 2015 году 85% производителей программного обеспечения использовали открытый исходный код (opensource), и 70% программного обеспечения – компоненты с открытым исходным кодом.*

Сканеры кода были весьма дорогостоящими и требовали вложениях серьезных ресурсов от самого заказчика, поэтому позволить их себе могли преимущественно крупные компании. Позже стала популярна методология непрерывного деплоя, увеличилась доля opensource, произошел ряд громких событий, связанных с эксплуатацией и обнаружением уязвимостей. Это привело к переосмыслению разработчиками подхода к безопасности реализуемых программных проектов.

Немаловажно, что практика написания программ посредством копирования фрагментов открытого кода перестала быть распространенной. Сейчас используются целостные артефакты и библиотеки, а это, в свою очередь, снизило потребность поиска фрагментов кода. И сегодня уже требуется такой инструмент, который позволяет обеспечивать безопасность кода и управлять лицензионными рисками в условиях agile-разработки – инструмент из класса систем SoftwareCompositionAnalysis (SCA). SCA, в отличие от сканеров кода, доступны каждому, не только крупным компаниям.

Ценность систем SCA в том, что они позволяют обнаруживать уязвимости компонентов и/или управлять лицензионными рисками. При интеграции с инструментами разработки, могут применяться политики SCA, чтобы автоматически блокировать проблемные компоненты до добавления их в проект. Наиболее мощные решения в этом сегменте представлены производителями Black Duck Software(поглощенный компанией Synopsys), White Source Software, Sonatype, Flexera и Veracode. Некоторые из этих вендоров сделали акцент на управлении лицензионными рисками, другие – на вопросах безопасности. Система непрерывного управления открытым ПО имеет возможности автоматизации на протяжении всего цикла разработки ПО, начиная со стадии выбора компонентов и заканчивая отслеживанием компонентов после выпуска релиза.

При выборе подходящего инструмента для управления opensource, обычно фокусируют внимание на следующих вопросах:

- Инвентаризация компонентов
- Непрерывное обнаружение уязвимостей
- Управление лицензионными рисками
- Возможности «ShiftLeft» и автоматизация

Первый шаг в организации контроля за уязвимостями открытого кода и лицензионными соглашениями – инвентаризация бинарных компонентов и исходного кода opensource в вашем программном продукте. Для качественной инвентаризации важно, чтобы в решении SCA базы известного opensource активно обновлялись.

Следом возникает вопрос: где наиболее оптимально было бы обрабатывать полученные отчеты – в облаке или в собственном ЦОДе? Для одних компаний предпочтительнее SaaS-решение по подписке – ведь это безопасно, удобно, можно быстро начать использование продукта. Для других компаний критично, чтобы никакая информация об используемых компонентах и их проектах не покидала корпоративные границы. В таком случае требуется on-premise решение, которое развертывается в корпоративном ЦОДе. После того, как инвентаризация всех применяемых компонентов opensource проведена, необходимо получить информацию о рисках их применения.

Один компонент – угроза системе

Ежегодно сообщается о сотнях уязвимостей компонентов открытого кода. Киберпреступники понимают, что уязвимость в одном компоненте может помочь им скомпрометировать большое количество систем. Необходимо проводить тщательную проверку безопасности загруженных библиотек и исходных кодов. Чем больше источников информации об уязвимостях используется и профессиональнее команда исследователей вендора проверяет эту информацию, тем меньше будет ложных срабатываний и качественнее результат проверки вашего ПО.

Выявить уязвимости – это только половина задачи, нужно ведь еще принять ответные меры. Для ускорения процесса разработки, развитые системы SCAпозволяют автоматизировать формирование безопасного локального репозитория и выдачу рекомендаций разработчикам по устранению обнаруженных уязвимостей. Так вы можете существенно экономить время разработчиков и специалистов по безопасности.

Интервью для телеканала РБК

Уже после выпуска релиза вашего ПО могут обнаруживаться новые уязвимости. Система должна уметь отслеживать компоненты не только на этапе создания продукта, но и на всем его жизненном цикле. После выпуска релиза важно, чтобы вы как можно скорее узнавали об уязвимостях в вашей разработке.

Оценка риска нарушения лицензионных соглашений больше не является только лишь частью юридических процедур в ходе слияния и поглощения крупных компаний или при выходе на IPO. Постепенно это становится обычной процедурой перед каждый релизом ПО. Следовательно, юристам требуется автоматизированное решение для управления рисками лицензионных соглашений открытого кода, чтобы идти в ногу с непрерывным деплойментом программных продуктов.

Отслеживание лицензий открытого кода в разрабатываемом продукте усложняется из-за роста количества типов лицензий открытого ПО, множественности версий и ошеломляющего объема кода, опубликованного без упоминания лицензий. Системы SCA помогут при управлении лицензионными рисками путем автоматизированного создания отчетов правовой оценки с перечнем лицензий для юридического отдела и путем применения лицензионной политики во время цикла разработки ПО.

Чем раньше – тем лучше

Чем раньше обнаруживается проблемный компонент, тем легче и дешевле заменить его. «Раннее обнаружение», так называемое «ShiftLeft» заключается в проведении оценки ПО на наиболее ранних стадиях процесса разработки, что позволяет обнаруживать проблемы тогда, когда их легче и дешевле устранить. Opensource с критичной уязвимостью или неподходящими условиями лицензионного соглашения перед добавлением в свой репозиторий, сборку или даже перед началом тестирования ПО позволит повысить производительность ценных специалистов и улучшить качество вашего реализованного проекта.

В системах управления opensource для реализации «ShiftLeft» и автоматизации предусмотрены инструменты анализа компонентов перед загрузкой, предупреждения о проблемах качества и безопасности opensource в режиме реального времени, имеются возможности интеграции со средой разработки – репозиториями, системами сборки и CI-серверами. Развитые SCAне просто оповещают о проблемах, но и имеют инструменты выбора альтернативных более подходящих компонентов.

Автоматизация – краеугольный камень CI/CD, при этом автоматизированная система управления открытым ПО является критически важным элементом. Вручную невозможно обнаруживать проблемы с безопасностью, совместимостью и качеством в режиме реального времени. Автоматизация этих процессов не только защищает от человеческих ошибок, что повышает точность, но и ускоряет процесс разработки и экономит драгоценные ресурсы.

Ключевые возможности систем управления opensource в части автоматизации – блокирование использования проблемных компонентов, автоматическое применение политик, предупреждение об уязвимых и устаревших компонентах, развитый API для интеграции со средой разработки, включая баг-трекеры. Наглядные отчеты о рисках opensourcев проектах являются важным инструментом анализа эффективности SDLCдля руководителей.

Ценность систем управления opensource заключается в точном определении компонентов с открытым исходным кодом и их уязвимостей, автоматизации создания безопасного репозитория, автоматизации проверки компонентов opensource на всем цикле разработки и сопровождения ПО, и их лицензионных соглашений. Все эти возможности помогают сэкономить время ценных специалистов – разработчиков, тестировщиков, юристов, сотрудников отдела безопасности и управления рисками.

Вручную невозможно обнаруживать проблемы с безопасностью, совместимостью и качеством в режиме реального времени.