БЕЗОПАСНОСТЬ
КОРПОРАТИВНЫХ ПРИЛОЖЕНИЙ

Ak Kamal Security

СОДЕРЖАНИЕ

Перевод и подготовка материала проведены компанией Ak Kamal Security. Автором оригинального материала под названием “Securing Enterprise Applications” является компания Securosis (*www.securosis.com*).

ВВЕДЕНИЕ

Как аналитическая и исследовательская компания, сфокусированная на информационной безопасности, мы общаемся с компаниями из списка Fortune 1000 каждую неделю. И из наших бесед становится ясно, что большая часть этих компаний имеют заметные недостатки в их программах обеспечения безопасности, в частности, внутри и в окружении крупных корпоративных приложений, которые являются основной их бизнеса. Это удивительно, ведь такие платформы как SAP и Oracle активно используются уже более 10 лет и можно ожидать, что за это время все аспекты их безопасности более или менее проработаны. Это является неожиданностью и для самих компаний, которые всегда думали, что их процессы и инструменты достаточно защищены.

Есть много причин появления пробелов в безопасности. Но основными являются две – сосредоточенность основных средств обеспечения безопасности на защите сетей или платформ и общая неосведомленности о продуктах разработанных специально для защиты корпоративных приложений. К примеру, компании часто инвестируют в общие инструменты оценки, которые не обеспечивают углубленного управления и контроля корпоративных приложений. В некоторых случаях, компании ссылаются на сбор журналов действий всех приложений с помощью SIEM, но используемые подобными решениями методы сбора данных не позволяют собрать нужную информацию для адекватной оценки действий пользователей.

Но есть и дополнительные причины. Поставщики корпоративных приложений предоставляют рекомендации по защите по обеспечению безопасности, но не могут предложить к покупке реальные продукты для ее обеспечения и даже редко дают советы об удалении или отключении неиспользуемых компонентов приложений, что могло бы снизить площадь атак. Те, кто обеспечивают безопасность, в свою очередь, мало знают о работе этих приложений и не могут самостоятельно определить какая модель развертывания будет эффективной. IT-персонал также обычно не стремится делать лишнюю работу, а потому предпочитают делать только то, что от них требуют. Наконец, крупные предприятия зачастую избегают решений для контроля безопасности корпоративных приложений из-за страха, что эти системы могут нарушить работы приложения, уменьшить производительность или повлиять на удобство использования. Все эти причины способствуют появлению пробелов в безопасности корпоративных приложений.

Управление цепочками поставок, взаимоотношениями с клиентами, ресурсами предприятия, финансовыми операциями – все это включают в себя современные корпоративные приложения. Каждое предприятие зависит от них в организации бизнес-процессов и тратит огромные деньги на них и их поддержку. И эти корпоративные приложения нуждаются в обеспечении защиты для того чтобы защитить эти инвестиции, ведь хорошо известно, что эти приложения являются одной из главных целей атак, как со стороны инсайдеров, так и извне. Компании много инвестируют в эти приложения, в аппаратные платформы и сотрудников, которые должны будут обеспечивать их поддержку. И в большинстве реализаций инвестиции в безопасность данных проектов составляют лишь мизерную часть всего бюджета. Впрочем, для действительно крупных проектов 1-2 процента бюджета это огромные средства, поэтому однозначно говорить о том, что компании относятся к безопасности несерьезно, нельзя. Однако, эти инвестиции не всегда оптимальны – могут быть выбраны решения с ограниченной функциональностью, без

комплексного понимания доступных опций. В общем, пришло время взглянуть на все это по-новому.

В данном материале мы сфокусируемся на основных аспектах обеспечения безопасности корпоративных приложений и дадим практические рекомендации по повышению уровня их защиты. А также обсудим специфику обеспечения безопасности и соответствия требованиям в отношении крупных корпоративных приложений, выделим недостатки в защите и предложим подходящие решения и специфические инструменты, которые можно и нужно использовать в этих системах. Материал не претендует на исчерпывающий анализ контроля безопасности корпоративных приложений, а является, по сути, описанием общих недостатков защиты и базовых принципов обеспечения безопасности.

Рекомендуемые разработчиками средства контроля безопасности оставляют огромные пробелы в защите. Они не только не обеспечивают минимальное покрытие, но и влекут заметные расходы на повышение безопасности сетей, системы антивирусной защиты и антиспама, но эти и многие другие средства обеспечения безопасности используются для обеспечения комплексной защиты и не учитывают некоторые специфические моменты защиты корпоративного приложения. Большая часть разработчиков не имеют достаточных знаний о том, как работают платформы, в которых будут использоваться приложения, где и как будет собираться и анализироваться информация о событиях ИБ. В реальности, большинство разработчиков решений по информационной безопасности упрощают себе работу, концентрируясь на защите сетей и платформ вне приложения. В этом материале мы рассмотрим пробелы в обеспечении безопасности, и дадим специфические рекомендации.

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ ПРИЛОЖЕНИЙ. ПРИМЕРЫ

Ниже приведены основные варианты обеспечения безопасности корпоративных приложений на которые должны обратить внимание специалисты занимающиеся безопасностью и следящие за соблюдением требований. Мы будем использовать эти схемы при обсуждении пробелов в системах обеспечения безопасности, а также при сравнении того, как обычно организована защита в компаниях и тем, что должно быть для обеспечения лучшего контроля.

Соответствие требованиям

Соблюдение стандартов (например, PCI-DSS) и соответствие требованиям регуляторов остаются одним из основных драйверов при контроле безопасности корпоративных приложений. Большая часть этих требований сосредоточена на проверке базовых частей приложений, а по факту на оценке их конфигураций. Как правило, прежде всего контролируются права привилегированных пользователей (к чему они могут получить доступ), разделение обязанностей, общие политики безопасности, скорость применения патчей и взаимодействие приложений. Также важными моментами являются ведение журнала действий и непрерывный контроль соответствия, позволяющий аудиторам проверить систему в любой момент времени прошедшего с момента последнего аудита.

Управление изменениями и применение политик

Кроме внешних требований, в компании могут принять собственные политики безопасности с целью снижения рисков, повышения надежности приложений и уменьшения вероятности мошеннических действий. Эти политики будут регламентировать действия администраторов и снизят риски административного злоупотребления имеющимися привилегиями. Также данный пример включает в себя удаление ненужных модулей, отслеживание действий привилегированных пользователей, предупреждение (а возможно и блокирование) об использовании неподходящих элементов управления, отключение доступа IT-администраторам к данным приложения. Все это, естественно, специфично для каждой системы и гораздо сложнее, чем просто оценка приложений для выполнения требований и стандартов. Эффективный контроль всего этого требует сочетания оценки, безостановочного контроля и анализа журналов событий.

Безопасность

Разговоры о том кто представляет наибольшую угрозу безопасности – внешние злоумышленники или инсайдеры – не утихают уже 15 лет. Но для корпоративных приложений этот вопрос неактуален – здесь обе эти группы представляют одинаковую угрозу. Более того, внешний злоумышленник вполне может действовать как привилегированный инсайдер, в том случае, если получит необходимый уровень доступа. Поэтому необходим постоянный неусыпный контроль за проводящимися операциями – и не просто контроль (отслеживать миллионы действий в реальном времени, не выделяя какие-то сомнительные моменты бессмысленно), а анализ с определенным сводом правил. И конечно, этот контроль должен быть непрерывным. Но эта возможность

не предлагается в приложении и может быть обеспечена либо сторонними инструментами, например, от поставщика платформы.

Подтверждение транзакций

Чем больше корпоративных приложений становятся доступными для внешних пользователей, тем более серьезно стоит проблема мошенничества. Каждый web-сервис сталкивается с разнообразными атаками, которые могут позволить злоумышленнику инициировать фиктивные транзакции, получить частичный контроль над поддерживаемой базой данных, что приведет к ошибкам. Но в отличие от общих угроз безопасности, эти атаки спланированы так, чтобы мошеннические транзакции выглядели как обычный трафик. Как компании отслеживают эту ситуацию? Некоторые компании используют собственные макросы или процедуры для поиска ошибок постфактум. Другие используют сторонние средства мониторинга и системы обнаружения атак в реальном времени. Эти решения разработаны для того, чтобы выявлять необычные действия пользователей в приложении, используя метаданные, эвристический анализ и атрибуты пользователя/устройства.

Использование конфиденциальных данных

Большая часть компаний контролирует использование конфиденциальных данных. Это может быть требованием регуляторов, платежных систем или быть определено внутренними политиками безопасности. Стандартный набор ограничений на доступ к ним включает: ограничение доступа к личным данным IT-администраторов, ограничение на одновременную выдачу большого количества данных, а также попыток получить однотипные данные, вроде номеров платежных карт. Кроме того, имеется распределение ролей пользователей, которое учитывает потребности разных групп пользователей, применяя к ним дополнительные ограничения, не отменяя общие. Все это сделано с целью выявления нестандартного поведения, информирования о нем, а также блокировки действий, которые выглядят подозрительными. Подобный контроль может быть частью приложения, но чаще всего включен в логику базы данных или представлен в виде отдельного решения для мониторинга/маскировки данных в качестве обратного прокси для базы данных.

ПРОБЕЛЫ В БЕЗОПАСНОСТИ

Корпоративные приложения, как правило, имеют конкретную бизнес-функцию: управление цепочками поставок, отношениями с клиентами, эффективностью бизнеса и так далее. Они могут поддерживать тысячи пользователей, быть связанными с другими платформами, но это специализированные приложения очень высокой сложности. Их разработка занимает много лет для разработчиков, а IT-персонал тратит очень много времени на то, чтобы понять все нюансы функционирования приложения, его компонентов, настройки и того как выглядят те или иные операции.

Средства обеспечения безопасности также зачастую бывают специализированными – сосредоточенными на определенном виде анализа. Например, средства обнаружения вредоносных программ применяются в определенных сценариях, выявляя вредоносы при контроле сетевых потоков, файлов или журналов отчетов. Но очень редко эти инструменты фокусируются на обнаружении угроз безопасности на уровне приложений. Они, как правило, используются шире, покрывая всю IT-инфраструктуру. А те, что все же обращают внимание на уровень приложений, чаще всего слабо представляют принципы и особенности функций приложения, особенно если речь идет о таких сложных комплексных платформах, как Oracle Peoplesoft систем SAP ERP.

Если вы используете корпоративные приложения SAP или Oracle, то можете быть уверены, что в вашем распоряжении есть достаточное количество инструментов безопасности. Большая часть разработчиков предлагают встроенные средства журналирования, идентификации и шифрования. Но даже они во многих случаях не могут закрыть все пробелы в безопасности, так как в основном ориентированы на выявление ошибок и решение проблем производительности.

Разработчики средств защиты, "на словах" понимают, что такое уровень приложений, но их компетенция обычно заканчивается на уровне порта сетевой службы. Общие события и конфигурации вне приложения они еще могут покрыть, но внутренние нет. Давайте разбираться на конкретных примерах:

Понимание использования приложений

Самое главной и наиболее остро ощущаемой является проблема непонимания структуры корпоративных приложений системами мониторинга. Для непрерывного мониторинга необходимо не только собирать необходимые данные, но и понимать их. И это серьезная проблема, ведь точки сбора данных, равно как и их "язык" заметно отличается от платформы к платформе. Например, для мониторинга платформы SAP система должна понимать ее операционные коды (так называемые Tcodes), которых более 100 тысяч. Во-вторых, должно быть понимание точек сбора этих данных – журналы мониторинга приложения и базы данных не обеспечивают достаточный объем информации. В качестве другого примера приведем Oracle – ее приложения полагаются в основном на процедуры внутри базы данных. Инструменты мониторинга позволяют видеть имя процедуры и набор переменных в запросе пользователя. Но если вы не знаете, что за процедура выполняется, то понятия не имеете, что действительно происходит в данный момент.

И вновь приходится контролировать связь между приложением и базой данных. Так как журналы событий не дают полную картину ситуации, нужно выяснять, что обозначает тот или иной код или процедура запроса.

Традиционные разработчики систем безопасности заявляющие о глубокой инспекции пакетов используют механизмы обучения для того чтобы понять каким образом приложение работает. Многие используют для этого метаданные (в том числе, пользовательские, приложения, данные о времени суток и геолокации) собранные в сети, возможно вместе с чем-то вроде кодов SAP для того чтобы оценить используемые запросы. Эти запросы собираются и анализируются с целью создать некую модель "нормального" поведения и действий в приложении. Но обнаружить мошенничество или злоупотребления при таком подходе предельно сложно. Хотя, данный подход и эффективен при расследовании инцидентов и для общего контроля. Кроме того, этот подход позволяет генерировать ложные положительные события. Продукты, изначально созданные для обеспечения безопасности корпоративных приложений и баз данных, на самом деле гораздо более эффективны благодаря лучшему пониманию целевого приложения. Разработка таких продуктов для мониторинга приложений весьма сложна. Но только понимание внутренней структуры приложения и используемых запросов, позволяет сосредоточить свое внимание на самых уязвимых местах, к примеру, на моменте ввода заказа, который часто используется инсайдерами для мошенничества. Такой подход позволяет более эффективно и оперативно реагировать на несанкционированные действия, уменьшает необходимый для анализа объем данных и упрощает работу службы информационной безопасности.

Состав приложения

В этом исследовании часто упоминается термин "базы данных". Базы данных служат для хранения, поиска и управления данными приложения. Каждое корпоративной приложение опирается на какую-либо базу данных. Но и сами базы данных представляют собой достаточно сложные приложения. Для обеспечения безопасности корпоративного приложения и выполнения требований необходимо решить многие вопросы по защите баз данных и платформ.

Также важно помнить, что не бывает готовых корпоративных приложений "из коробки". Каждое приложения подвергается заметной модификации под клиента, причем, зачастую, не на уровне настроек и модулей, а на уровне кода. Эти изменения делаются по разным причинам исходя из потребностей клиента и необходимости обеспечения взаимодействия с другими приложениями. В то же время, несмотря на то, что при внесении изменений в код используется статический и динамический анализ на наличие уязвимостей, сами представители компаний признают, что эти изменения все же снижают безопасность базового приложения.

Развертывание и настройка

Практически невозможно встретить два корпоративных приложения, которые развернуты одинаково, имеют аналогичный функционал и конфигурацию. Все приложения адаптированы в соответствии с набором требований и спецификой деятельности той или иной компании. Все это заметно усложняет сканирование и поиск уязвимостей. Кроме того, приложения и базы данных заметно отличаются друг от друга окружением – операционными системами, сетевыми

решениями, что также не упрощает задачу. Это оказывает влияние как на принцип сбора информации, так и на определение набора правил. Все продукты мониторинга способны оценить состояние и найти недостатки в приложении, основываясь на списке известных уязвимостей и проблем. Но этот подход работает только с приложением "из коробки" и фактически основывается только на информации о его версии. Понимание реально работающих приложений требует более пристального внимания. К примеру, тестовые приложения зачастую имеют бэкдоры, которые затем эксплуатируются атакующими. И информация о версии в данном случае будет недостаточно, ведь уязвимость может быть и в каком-то из модулей. В таком случае поможет только тщательный анализ программного обеспечения. Распределение обязанностей между приложением, базой данных и IT-администраторами также не может быть определен путем сканирование сетевого порта или даже подключения LDAP – это требует постоянного опроса приложения и накопления данных. Недостатки конфигурации сети, слишком простые пароли и публичные аккаунты легко обнаружить с помощью обычных сканеров, конечно при условии, что они имеют правильные настройки. Но сканеры не помогут определить права собственности на данные, настройки доступа к файлам, работоспособность систем аудита и десятки других известных проблем.

Сбор данных является второй важной проблемой. В большинстве случае для получения оценки приложения используется сканер портов, особенно в случаях, где использование агентов нежелательно. Этот способ является достаточно удобным и не требует вмешательства в систему. Сканеры приложений занимаются поиском специфических настроек приложений на дисках и в базе данных. Такая проверка может проводиться как по инициативе агента на платформе приложения, так и удаленно через подключение защищенное SSL/TLS. Мы называем это "аккредитованное сканирование", потому как данный метод требует доступа к файловой системе или базе данных, а иногда и того, и другого. Естественно, для того, чтобы получить полную оценку, нужно собрать данные и системы и базы данных. Но сканеры общего назначения в любом случае не позволят вам получить более трети от общей массы необходимой информации. Только специализированные сканеры для корпоративных приложений и баз данных позволят собрать 70-100 процентов необходимых данных в зависимости от способа сбора информации и применяемых политик.

Циклы обновления приложений

Если у вас есть iPhone или любой другой продукт компании Apple, то вы получаете уведомление об обновлении одного или нескольких приложений ежедневно. Корпоративные приложения обновляются не в пример реже, несмотря на то, что ставки здесь гораздо выше. Достаточно распространенная практика, когда обновления безопасности не устанавливаются до полугода. А если это действительно большая система SAP или Oracle, то зачастую ее не обновляют до года. И проблема не в том, что администраторы не игнорируют проблему или не понимают, а в том, что критические патчи безопасности могут повлиять на работоспособность приложения, что в свою очередь приведет к финансовым потерям. Кроме того, остановка приложения требует максимальной мобилизации всех занимающихся ее поддержкой, а работа компании на это время фактически парализуется. При этом вероятность атаки злоумышленника не столь вероятна. Как результат, после оценки рисков чаще всего принимается решение о тщательном тестировании патча безопасности на резервной системе до тех пор, пока не будет уверенности в том, что он не повлияет на работоспособность системы и всех подсистем, и лишь после этого принимается решение о применении его в "боевой" системе.

Из-за невозможности быстрого применения обновлений, многие компании ищут обходные пути для устранения известных уязвимостей. И многие из этих методов оказываются достаточно эффективными, хотя и не столь эффективными как традиционные обновления. Часто для этого используются блокировки, ограничение доступа в сеть, ручное вмешательство в процессы и так далее. Хорошей новостью является то, что некоторые компании ускорили процесс внедрения обновлений, используя современные технологии – виртуализацию и облака. Некоторые устанавливают обновление лишь на некоторые серверы, работающие в режиме балансировки нагрузки, с постепенной установкой обновления на все новые узлы, но с возможностью отказа от обновленных серверов в случае проблем с обновлением. Другие используют облачные сервисы и виртуализацию для того чтобы развернуть два набора "боевых" серверов – обновленный и необновленный, с возможностью быстрого "отката" на гарантировано работоспособную версию. Но, к сожалению, данные механизмы пока не слишком распространены.

События приложений и сбор логов

Как уже говорилось ранее, логи баз данных и приложений, как правило, не ориентированы на обеспечение безопасности, а предназначены для IT-персонала, который по их показаниям диагностирует неисправности, выявляет ошибки и проблемы с производительностью. Но при этом в них часто нет информации о многих специфических событиях, в том числе действиях администраторов. Кроме того, они зачастую лишены достаточного количества параметров фильтрации, что не позволяет оперативно выявлять необходимые события, которые просто теряются в огромном потоке информации. Во многих случаях информация с логов может быть собрана с помощью SIEM, но подобным системам зачастую нехватает понимания данных о событиях конкретных приложений. Но реальной проблемой является производительность – сбор логов приложения обычно увеличивает нагрузку на платформу на 10-20 процентов, а сбор логов с базы данных и вовсе на 20-40 процентов, что, как вы понимаете, недопустимо для многих компаний.

Для эффективного мониторинга, оценки и аудита корпоративных приложений, вам, вероятно, придется создать собственные инструменты или использовать сторонние продукты для того, чтобы расширить те возможности, которые у вас имеются. Поставщики платформ знают, как правильно собирать информацию со своих платформ, но готовят свои решения для экспертов по работе с их системами. Обычные системные администраторы, аудиторы, специалисты по информационной безопасности и другие IT-администраторы зачастую не имеют достаточной глубины знаний для работы с этими инструментами. При этом, как уже говорилось, поставщики не предоставляют достаточной информации о своих системах, а также не рекомендуют сторонние продукты, которые могли бы помочь.

РЕКОМЕНДАЦИИ

Целью этого документа является не полное изучение всех аспектов безопасности корпоративных приложений, а обзор недостатков в ядре самого приложения. Мы уже указали на основные пробелы в безопасности и недостатки в реализации, а теперь пришло время рассказать о том, как их устранить. Мы делим наши рекомендации на две части: основные элементы текущей системы безопасности, которые можно использовать более эффективно и возможности безопасности, которые должны быть частью системы.

Основные элементы программы

Идентификация и управление доступом. Идентификация и авторизация являются первой критической линией защиты системы безопасности вашего приложения. SAP, Oracle и другие разработчики корпоративных приложений предлагают инструменты идентификации и управления доступом, которые позволяют разграничить доступ пользователей в зависимости от их статуса и должностных обязанностей. Разграничение доступа является очень важной частью системы безопасности, но поставщики обычно обеспечивают вполне достаточные возможности для гибкой настройки доступа внутри платформы. Но есть платформы, которые обслуживающие несколько торговых точек, а также те, которые используют для доступа некие общие идентификаторы, в том числе выданные государством, могут быть весьма интересны злоумышленникам. А потому, максимум внимания должно уделяться введению четких правил авторизации в поддерживаемой базе данных, а так же контроль прав доступа пользователей в реальном времени.

Пароли

Парольная защита не очень хорошая для обеспечения безопасности и даже требование регулярной смены паролей не дает действительно надежной защиты, лишь повышая неудобство работы с системой. Фишинг – эффективное средство получить пароли пользователей, что позволяет злоумышленникам получить доступ к системе. Поэтому мы рекомендуем использовать двухфакторную аутентификацию, как минимум для административного доступа. Решения для добавления второго фактора аутентификации вполне доступны и достаточно легко интегрируются с приложениями и позволяют заметно повысить безопасность привилегированных учетных записей.

Мобильность

Защита ваших пользователей, использующих ваши компьютеры в вашей сети под защитой вашего фаерволла – это прошлый век. Мобильные устройства, представляют собой современное и распространенное решения, которое может обеспечивать доступ к вашему корпоративному приложению. Большинство пользователей не собираются ждать, когда ваше специалисты подготовят устройства и определят их политики – они просто покупают его и начинают использовать. Именно поэтому мобильные устройства нужно изначально считать существенным расширением для вашей традиционной экосистемы. Для них необходимо тщательно продумать механизмы идентификации пользователя в сети, сохранив функциональность устройства за пределами вашей сети, а также возможность временной приостановки активности устройств.

Возможно, стоит задуматься о введении карантина для данных и приложений на устройстве. В идеале, должно использоваться облачное решение по идентификации на основе токенов, а также приложение для контроля мобильного устройства, должны быть важной частью стратегии безопасности корпоративного приложения.

Конфигурация и управление уязвимостями

С самого начала материала мы говорим о том, что одной из главных особенностей корпоративных приложений является сложность сбора данных с приложения для обеспечения его адекватного мониторинга. При этом встроенные средства контроля – это уже две трети успеха в организации надежной защиты корпоративного приложения. Эти инструменты позволяют получить вполне достаточный объем данных соблюдении политик безопасности и действиях пользователей. Да, конечно, это может делать и сканер, но высока вероятность, что он будет пропускать гораздо больше важной информации, нежели специализированные инструменты. В общем, лучшим вариантом будет использовать тот продукт, который эффективно получает данные как из, так и извне приложения, совместно с правильными политиками безопасности. Куча разных политик безопасности является четким показателем, что вы используете неправильные инструменты. Настоящие сканеры правильно понимают структуру корпоративных приложений, таких как SAP или Oracle и позволяют вам интегрировать политики в сканер, для дальнейшего использования в системе.

Шифрование данных

Большая часть корпоративных приложений изначально имеет некоторые возможности шифрования. Причем возможны два варианта: либо приложение включает собственную библиотеку шифрования и систему управления ключами, либо полагается на шифрование базы данных. Но, как показала практика, только шифрования базы может быть недостаточно, кроме того, работа с зашифрованными в базе данными сложна в случае необходимости их пересчета и изменения. Ну и наконец, шифрование негативно влияет на производительность системы. В результате многие компании либо отказались от шифрования вообще, либо отказались от шифрования временных файлов таблиц с целью повышения производительности. К счастью, есть удобный вариант шифрования, который позволяет минимизировать риски безопасности, и почти не влияет на производительность – он работает на уровень ниже приложения и базы данных, шифруя информацию непосредственно перед записью на диск. Этот метод быстрее, чем шифрование на уровне полей в базе данных и безопаснее за счет того, что не требует внесения никаких изменений в само приложения. Этот подход также защищает резервные копии и защищает от возможности считывания данных непосредственно с диска IT-администраторами. Мы рекомендуем рассматривать разные продукты для шифрования от разработчиков приложения/базы данных, а также обратить внимание на продукты разработанные третьей стороной.

Безопасность сетей и межсетевые экраны

Если вы запускаете корпоративное приложение, то у вас скорее всего уже есть межсетевые экраны и системы обнаружения вторжений. А вполне возможно у вас используются NGFF, WAF или DLP для защиты приложения. Учитывая, что вы уже инвестировали средства в эти решения, нет сомнений, что вы будете стараться их использовать и для защиты корпоративного приложения. Но, к сожалению, в данном случае, все эти продукты малоэффективны, потому что они, опять

же, не понимают принципы работы приложения, ограничиваясь контролем сети и подключений. Кроме того, корпоративные решения все больше завязываются на облачные сервисы, что делает их еще менее эффективными. Мы рекомендуем присмотреться к специальным решениям для мониторинга приложений и шлюзам, которые созданы для максимально эффективного взаимодействия с корпоративными приложениями и умеющими реагировать на специфические атаки, совершаемые на корпоративные приложения. Мы не предлагаем избавляться от существующей инфраструктуры, обеспечивающей безопасность сетей, а лишь говорим о том, что есть более эффективные способы защитить ваше приложение.

Сбор логов и журналы аудита

Вам необходимо собирать логии для того чтобы оценивать использование системы. Но большая часть решений просто собирают все имеющиеся данные, не выделяя важные события, что не позволяет выбрать действительно важные с точки зрения информационной безопасности события. Причем, обсуждать это с разработчиками SIEM сложно – выделение важных событий требует пристального внимания с их стороны и значительных доработок. Мы уже упоминали о том, что корпоративные приложения заметно отличаются от других и их логи не предназначены для обеспечения безопасности и аудита. Поэтому многие пользователи просто отключают встроенную систему ведения журналов событий, используя вместо нее регистрацию событий в сети. Есть несколько причин не идти по этому пути. Во-первых, разработчики корпоративных приложений, наконец, стали понимать, что ИБ логи приложений нужны больше чем IT, и стали делать шаги по повышению информативности и улучшению фильтрации событий. Во-вторых, использование систем разработки сторонних компаний делает достаточно сложным сбор и фильтрацию большого числа событий с приложения и базы данных. Ну и наконец, некоторые типы данных могут быть неправильно проанализированы и скореллированы не с теми событиями. Конечно, современные решения для сбора данных обладают все большей производительностью, позволяют работать с “большими данными”, а также научились накапливать информацию о некорректных действиях за долгий срок для улучшения анализа. По факту проблема все же имеет место быть, но со временем становится менее критичной и если у вас есть необходимость в сборе логов, то она вполне может быть удовлетворена современными средствами при правильном их применении.

МОМЕНТЫ, КОТОРЫЕ УПУСКАЮТСЯ ИЗ ВИДА

Контроль корпоративных приложений

Непрерывный контроль активности корпоративного приложения с пониманием принципов его работы, является одним из главных пробелов в обеспечении его безопасности. Мониторинг активности приложения и базы данных должен, как минимум, обеспечивать захват и запись всей активности приложения (включая действия администратора) в реальном или близком к реальному времени, даже в том случае, когда приложение развернуто на нескольких платформах, и предупреждать и/или блокировать действия, нарушающие политики. Инструмент для удаленного контроля событий приложения, должен обеспечивать сбор данных с разных источников и централизованное хранение для последующего анализа. Считайте, что это некая смесь SIEM и IDS. Она должно иметь возможность правильно понимать события в приложении до уровня транзакций и уметь проводить анализ событий разными методами (включая эвристический анализ, исследование метаданных, поведение пользователя, атрибуты, черные и белые списки команд). В идеале платформе должны быть понятны все особенности работы приложений для обеспечения максимально эффективного обеспечения безопасности. И важный момент: осуществление не только мониторинга событий, но и возможности блокирования действий. Правильно сконфигурированные белые/черные списки помогут предотвратить использование уязвимостей нулевого дня и другое нежелательное поведение.

API шлюзы

Большие компании зачастую используют некие внутренние приложения, которые для работы с клиентами имеют web-интерфейс. Причем многие из этих приложений были разработаны и запущены еще до появления интернета и, соответственно, не учитывали большую часть ключевых моментов безопасности. Благодаря тому, что через web-интерфейс обеспечивается практически прямой доступ к внутренним ресурсам, такие системы с точки зрения безопасности просто катастрофа. Также в последнюю пару лет для организации безопасного доступа удаленных пользователей – в частности, для мобильных приложений – некоторые компании используют API-шлюзы. Они предлагают абстрактный уровень аналогичный функциям внутренних приложений для распространенных современных программных интерфейсов: RESTful API. Такой шлюз позволяет контролировать версии клиентов, взломанные устройства, а также поддерживать соответствие политикам, обнаруживать возможные случаи мошенничества и использовать систему аутентификации с использованием токенов. Если у вас в планах есть обеспечение поддержки удаленных пользователей, мы рекомендуем обратить внимание именно на такие шлюзы, а не полагаться на межсетевые экраны и модель безопасности, основанную на фильтрации трафика.

Тестирование на проникновение

Тестирование на проникновение незаменимая вещь для оценки безопасности корпоративного приложения, так как позволяет взглянуть на систему с другой – атакующей стороны. Только тест с моделированием реальной атаки позволит найти те бреши в системах безопасности корпоративного приложения, которые остаются вне зоны внимания разработчиков и сотрудников отдела информационной безопасности. Автоматические сканеры не позволяют провести полноценную оценку безопасности, так как корпоративные приложения содержат огромное

количества уникального кода и, как следствие, уникальных уязвимостей. Безусловно, проведение грамотного тестирования на проникновение стоит немалых денег, но, тем не менее, такое тестирование должно быть регулярным, так как любые обновления приложения и появление новых объемов кода может породить новые уязвимости. И даже если оплата качественного тестирования на регулярной основе вам не по карману, имеет смысл проводить хотя бы регулярную инструментальную проверку.

ЗАКЛЮЧЕНИЕ

Приведенные в этом материале рекомендации по обеспечению безопасности достаточно универсальны для любых систем. Мы призываем вас пересмотреть свою программу безопасности в свете описанных нами замечаний и свежим взглядом оценить ситуацию с безопасностью корпоративного приложения. Даже обеспечение профилактического контроля и мониторинга в режиме реального времени позволят в значительной мере повысить уровень безопасности. Мы понимаем, что некоторые из рекомендаций требуют затрат, но также прекрасно понимаем и то, что дополнительные бюджеты получить всегда непросто, а потому старались предложить альтернативные варианты или автоматизированные решения, которые в перспективе окупятся за счет уменьшения нагрузки на офицеров ИБ. А кроме того, эти рекомендации вполне можно использовать для корректировки имеющегося бюджета с целью обеспечить более надежную защиту приложений с меньшими затратами, отказавшись от покупки не самых эффективных и полезных продуктов и систем.

О НАС

Компания Ak Kamal Security, основанная в 2006 году, специализируется на разработке, поставках, внедрении и сопровождении средств криптографической защиты информации. Продукция компании, а также наших партнеров, среди которых крупные игроки на рынке информационной безопасности, покрывает практически весь спектр задач по обеспечению безопасности, стоящих перед бизнесом и другими структурами, для которых критично сохранение конфиденциальности данных и обеспечение безопасности бизнес-процессов.

Одним из важнейших преимуществ компании является географическая близость к нашим клиентам, знание специфики казахстанского рынка и особенностей законодательства в сфере информационной безопасности. Кроме того, это позволяет нам быстро реагировать на все запросы клиентов касающихся наших разработок – будь то обеспечение технической поддержки, или пожелания по улучшению и расширению функционала в соответствии со спецификой их пользования в каждом конкретном случае.

Обратившись в Ak Kamal Security, Вы найдете в нашем лице надежного и компетентного партнера и консультанта по вопросам информационной безопасности. Накопленный опыт и прочные партнерские отношения с ведущими производителями средств защиты информации, профессиональный подход к решению любых вопросов в этой сфере, а также внимательность к запросам клиента – гарантия высокого качества нашей работы.

Ak Kamal Security

КОНТАКТЫ

ТОО «Ak Kamal Security», г. Алматы, ул. Каблукова, 257
Тел: +7 (727) 381-05-26, +7 (727) 222-00-92
Факс: +7 (727) 381-00-39
Mail: info@akkamal.kz
Web: www.akkamal.kz, www.e-security.kz, www.mysign.kz