О безопасности SOA в корпоративной среде

Сегодня наблюдается заметный рост интереса к концепции сервис-ориентированной архитектуры (Service-Oriented Architecture, SOA), все большее число компаний внедряют проекты на основе SOA с целью уменьшения общих затрат на ИТ, многие поставщики ПО прилагают серьезные усилия по продвижению этого подхода. Ведущий специалист компании Cisco по информационной безопасности Алексей Лукацкий рассказывает о применении новейших сетевых технологий Cisco в качестве инструмента защиты SOA-ориентированной корпоративной информационной системы организации.

Идеологию сервис-ориентированной архитектуры зачастую преподносят в качестве революционного прорыва в области разработки программного обеспечения. Однако это не совсем так. Концептуально подход остался тем же, что и в процедурном или объектно-ориентированном программировании, только в SOA ушли от процедур к сервисам и от технологий к бизнесу. И согласованная работа корпоративных приложений обеспечивается именно сервисами.

Сервисы в рамках архитектуры SOA – это промежуточный уровень, благодаря которому становятся прозрачными любые изменения, происходящие как на уровне приложений для инфраструктуры, так и на уровне инфраструктуры для приложений. Особенность таких сервисов в том, что они имеют стандартизованный вход и такой же стандартизованный выход, что позволяет без проблем менять их на другие аналогичные сервисы, не боясь снижения эффективности всего решения в целом. И даже больше. Многократное использование таких сервисов, имеющихся в единственном экземпляре, позволяет быстрее адаптироваться к изменениям: модифицировать единственную копию сервиса гораздо проще, чем похожие фрагменты или объекты, разбросанные по разным приложениям, поскольку изменения касаются сразу всех приложений, использующих этот сервис (рис. 1).

Раньше (хотя иногда такой подход можно встретить и сегодня) SOA продвигалась главным образом разработчиками бизнес-приложений (Oracle, SAP, IBM и другими), но сегодня специалистам очевидно,

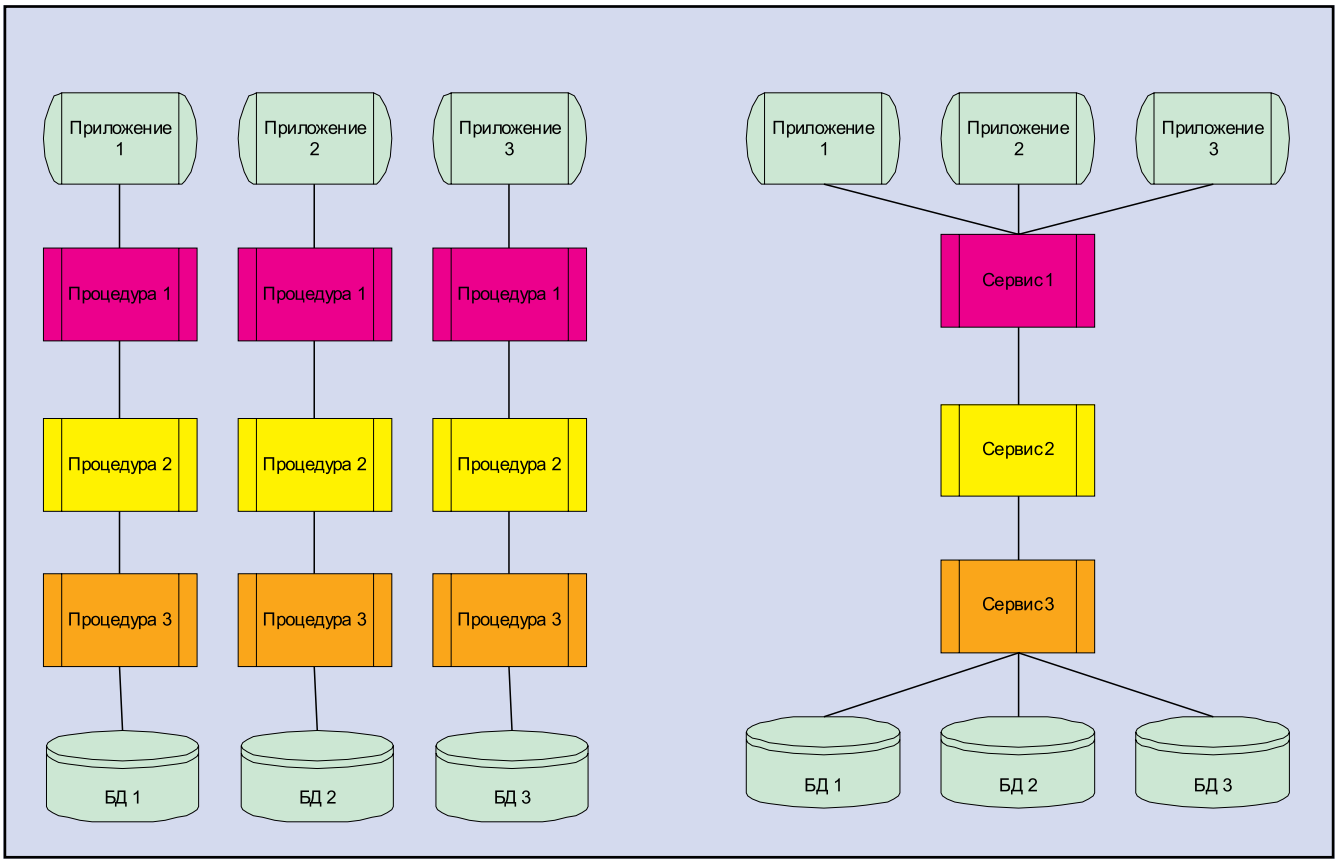

Рис. 1. Пример инфраструктуры ДО и ПОСЛЕ перехода к SOA

что добиться всех преимуществ этой архитектуры только за счет приложений невозможно. Во всех без исключения проектах ее построения присутствует сетевой уровень, с помощью которого и осуществляется взаимодействие разрозненных компонентов SOA, возможности которого задействованы не полностью. Ориентация только на приложения приводит к "утяжелению" ПО, так как, например, такие ресурсоемкие процессы, как маршрутизация сообщений, сетевое оборудование способно делать гораздо эффективнее. Так же, как и многие другие вещи: поддержку различных стандартов, интерфейсов, Web-сервисов, разгрузку серверов, балансировку нагрузки и т.д. То есть имеет смысл передать сети то, что она умеет делать лучше.

Очень часто под SOA-ориентированной системой понимается набор Web-сервисов, разработанных при помощи стандартизованных протоколов SOAP, XML, WSDL и других. И хотя SOA может быть реализована с использованием и других технологий – DCOM, CORBA, RPC и т.д., сегодня именно Web-сервисы наиболее часто употребляются для реализации данной архитектуры. Именно их мы и будем рассматривать далее с точки зрения информационной безопасности.

Об XML с точки зрения безопасности

Как обычно создаются те или иные технологии? Сначала возникает потребность в улучшении того или иного процесса или реализации той или иной задачи. Потом создается технология, затем появляются сообщения об огромном количестве дыр, и начинается процесс их "затыкания". Так рождаются технологии защиты. Web-сервисы и протокол XML изначально создавались не с точки зрения безопасности, а с целью организации взаимодействия приложений. Как следствие, вопросам безопасности должного внимания не уделялось. Разработка приложений и их безопасность – это две абсолютно противоположные вещи. Разработчик в первую очередь думает о красоте кода, о функциональности, о реализации тех или иных подходов и о концепции. Безопасник же ставит себя на место злоумышленника и рассуждает, что бы такого плохого он сделал на его месте. То же самое было и с протоколом XML. Те проблемы, которые в нем есть сейчас, могут привести к отказу в облуживании, возможности появления червей на базе XML, несанкционированному выполнению тех или иных команд, краже данных и т.п. То есть это проблемы, известные любому специалисту по защите, только в качестве их источника выбран новый протокол.

С 2003 года, по данным сообщества WebServicesSummit.com, стало известно о 13 тысячах уязвимостей в продуктах на базе XML. Но самое главное, что классические средства защиты, которые использовались ранее (те же самые межсетевые экраны или системы предотвращения атак) неспособны бороться с угрозами по отношению к этим уязвимостям. Не потому, что у них у самих есть недостатки, а потому, что они разрабатывались в другое время и совершенно для иных целей – для контроля преимущественно сетевого уровня. Вот здесь классические межсетевые экраны, сетевые антивирусы и т.д. работают идеально, поскольку они для этого и предназначены. С HTTP они уже работают хуже, а с протоколами SOAP и XML "классика" работает вообще из рук вон плохо.

О средствах защиты

Если обратиться к исследованиям Gartner, то станет понятно, что этот вопрос возник не сегодня. Еще в 2002 году аналитики указывали, что "Web-сервисы заново откроют 70 % путей для атак, ранее закрытых межсетевыми экранами, потому что Web-сервисы могут обойти традиционную защиту периметра, неся любую информацию в поле данных (то есть будучи по сути легитимными) и взаимодействуя с любым приложением в сети".

Одна из главных причин – открытие на межсетевом экране 80-го порта для работы с HTTP (именно на базе него работают XML, SOAP и Web-сервисы). Но классический межсетевой экран не "понимает", что такое Web-сервисы, он не "знает" о присущих им проблемах. Поэтому, открывая 80-й порт (или иной другой HTTP-порт) без должных средств защиты, мы впускаем в компанию (одновременно и выпускаем из нее) огромное количество проблем, связанных с теми самыми 13 тысячами обнаруженных уязвимостей, связанных с XML. Очевидно, что традиционных средств защиты становится в принципе недостаточно. Однако это не означает, что от них надо отказаться. Это говорит лишь о том, что необходимо использовать новые механизмы, которые расширяют традиционные средства безопасности.

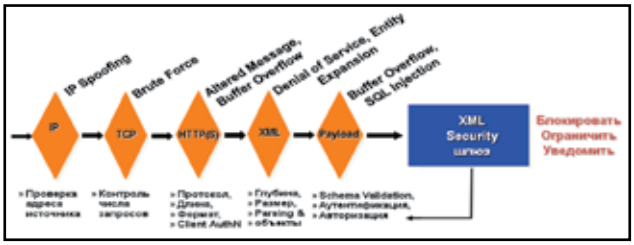

Рис. 2

Одним из таких механизмов является XML Security Gateway (рис. 2). Что это такое? Это программно-аппаратный комплекс, который выполняет несколько задач: ускорение и более эффективную обработку XML, разгрузку центральных процессоров серверов, масштабирование, управление и обеспечение безопасности. С точки зрения последней функции речь идет о полном анализе того, что происходит с XML в контексте безопасности.

Где место такого рода средств? Они могут быть установлены и в центре обработки данных (ЦОД), и на периметре сети, и в удаленном филиале. Главное, чтобы XML-трафик проходил через защитный XML-шлюз и мог быть им контролируем. Если посмотреть на инфраструктуру SOA, то станет понятно, что весь XML-трафик проходит через это устройство и на нем

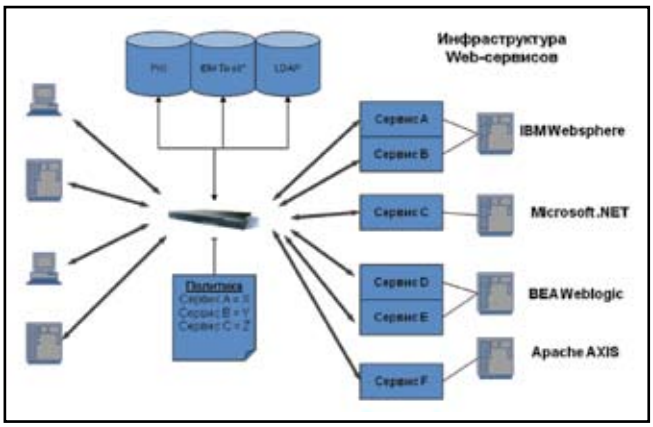

Рис. 3

реализуется политика безопасности Web-сервисов. То есть миновать это программно-аппаратное устройство сервисы не могут, а мы можем контролировать, что можно делать тем или иным пользователям и сервисам, а что нельзя. Поскольку мы работаем на едином стандарте XML, то нам абсолютно неважно, какие имеются приложения – это может быть BEA, Oracle, Microsoft или IBM (рис. 3).

Решения Cisco

В дополнение к продукции Cisco, обеспечивающей сетевую безопасность, появился специальный "слой", ориентированный на SOA, Web-сервисы и на взаимодействие приложений. Это – ACE XML Gateway и AON. Принцип работы первого решения был описан выше. А вот суть второго очень интересна.

Давайте посмотрим на то, как работает то или иное бизнес-приложение. Например, представим, что существует брокер, который работает с фондовой биржей. Есть приложение, которое принимает заявки на куплю-продажу акций. Есть также приложение, которое проводит эти сделки. На пакетном уровне (то есть там, где работают классические межсетевые экраны, маршрутизаторы и т.д.) все выглядит одинаково. Традиционные средства защиты не понимают разницы между работой приложений нашего брокера и передачей электронной почты или звонком по IP-телефонии. И там, и там передаются обычные IP-пакеты. И все, что мы можем сделать на этом уровне – защитить от атак типа "отказ в обслуживании", от перехвата трафика и каких-то стандартных сетевых атак. Поднявшись на уровень XML, мы повысим защищенность информационной системы, но только от технологических атак.

У нас нет возможности отследить, а имеет ли право данный пользователь осуществлять ту или иную транзакцию. И если перейти к более привычным для нас бизнес-процессам, например, электронному банкингу, – имеет ли право клиент перевести, например, более тысячи долларов в день? Ведь если приложение этого не контролирует, то злоумышленник, который перехватил идентификационные данные этого пользователя, сделает с его деньгами, что захочет.

Чтобы защититься от таких атак, нам необходимо анализировать бизнес-логику, то есть анализировать контекст взаимодействия именно в рамках Web-сервисов и бизнес-приложений. Поэтому помимо средств сетевой защиты, которые являются обязательными, но недостаточными, мы должны использовать решения, работающие с контекстом сообщений. Компания Cisco предлагает и такое решение – это AON (рис. 4).

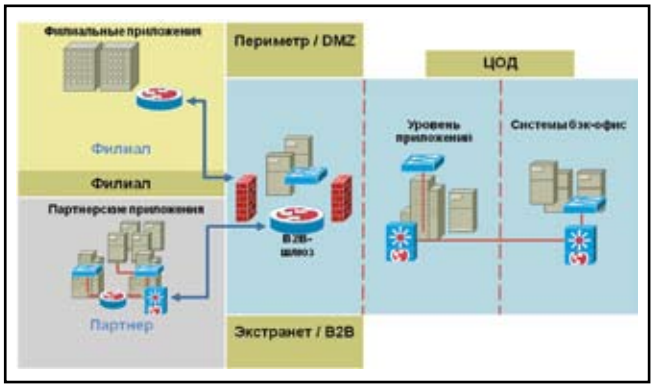

Рис. 4

Cisco AON предназначено для защиты бизнес-логики, по которой работают те или иные приложения. Все бизнес-транзакции между ними можно достаточно точно восстановить до вполне конкретных функций процессов: осуществлена отгрузка продукта такого-то, ордер на покупку акций или кадровый приказ. В результате чего возникает возможность оперировать языком бизнеса, а не терминами ИТ-технологий. Решение AON "понимает" этот язык.

Разумеется, Cisco не берет на себя задачу полного управления бизнесом, а только то, что касается сетевого уровня. Cisco контролирует: правомерна ли та или иная транзакция, не превышаются ли какие-либо лимиты, выполняется ли задача в срок. Само решение может быть выполнено в виде модуля для маршрутизатора Cisco ISR или коммутатора Cisco Catalyst, а также как специализированный программно-аппаратный комплекс, который обеспечивает максимальную производительность.

Заключение

Не раз уже говорилось и писалось, что о безопасности информационной инфраструктуры организации надо начинать думать не в процессе внедрения того или иного решения, а еще на этапе его проектирования. И сервис-ориентированная архитектура тут не исключение. Выбирая SOA-решение мы должны спрашивать его производителя не о количестве уязвимостей в его продукции, а о том, следует ли он циклу разработки ПО (SDLC) или нет. Отрицательный ответ на этот вопрос должен заставить задуматься, стоит ли тратить сотни тысяч долларов на незащищенное решение, которое может стать в будущем источником больших проблем. Но и получив утвердительный ответ, не следует забывать про самозащиту и использование средств защиты SOA-протоколов и сервисов безопасности.

Алексей Лукацкий, бизнес-консультант по безопасности, компания Cisco