УДК 621.391

И.Д. Медведовский, А.М. Поляков

ООО «Диджитал Секьюрити», Санкт-Петербург, Россия

АНАЛИЗ БЕЗОПАСНОСТИ БИЗНЕС-ПРИЛОЖЕНИЙ

Рассмотрено обеспечение безопасности корпоративных бизнес-приложений как одна из важнейших задач современного бизнеса. Проводится декомпозиция поставленной задачи, рассматриваются сферы применения выявленных подзадач, их достоинства и недостатки.

Ключевые слова: *безопасность бизнес-приложений.*

Введение

В этой статье систематизирован накопленный многолетний опыт по анализу защищенности бизнес-приложений после рассмотрения составных частей-подзадач, которые приходится неоднократно решать заказчикам в сфере применения бизнес-приложений. При этом все эти части-подзадачи решаются быстро и качественно при привлечении соответствующих специалистов.

Подзадача 1. Безопасность бизнес-приложений – проблема производителя

Взгляд с точки зрения руководства

Один из главных недостатков, который активно препятствует деятельности интеграторов, состоит в том, что безопасность бизнес-приложений это, прежде всего, проблема разработчика. Причем, когда речь идет об информационной системе в целом, состоящей из различных операционных систем, баз данных, приложений и т.д. – такой подзадачи не возникает. Очевидно, при наличии нескольких разных производителей предъявить всем претензии не представляется возможным. Кроме того, информационная система – это довольно сложный механизм, который требует регулярного анализа защищенности и, безопасность которого зависит от совокупности различных факторов. В случае же одной из систем управления предприятием или ключевого бизнес-приложения, когда производитель один, у руководства предприятия может возникнуть мнение, что безопасность – это проблема производителя. С технической точки зрения, это утверждение неверно, а с точки зрения руководства предприятия, оно, по меньшей мере, довольно простое и очень опасно его воспринимать, прежде всего, именно для деятельности предприятия. История не знает случаев, когда производитель нес ответственность за инциденты в области безопасности. Он продает лицензию на продукт и при этом не несет никакой ответственности за ущерб, который может возникнуть при использовании клиентом его продукта. Соответственно, вся многолетняя практика развития отрасли разработки программного обеспечения доказывает то, что для производителя вопросы безопасности его продукта имеют второстепенное, если не третьестепенное значение (на первом плане всегда только функционал). Это необходимо учитывать, когда речь идет о таких специфичных и малоизученных хакерами продуктах как, например, ERP, CRM, SRM и других специализированных бизнес-приложениях. Тем не менее, следует четко понимать, что безопасность приложения – это проблема руководства предприятия, которая не имеет отношения к производителю.

Взгляд с технической точки зрения

Проблемы безопасности делятся на следующие классы: программные, архитектурные, ошибки конфигурации и проблемы человеческого фактора. Если уязвимости, относящиеся к первому и, в некоторой степени, ко второму классу, имеют прямое отношение к производителю, то ошибки конфигурации и человеческий фактор – это те области, в которых наиболее часто возникают проблемы, приводящие к компрометации всей системы. В ходе выполнения работ по анализу защищѐнности бизнес-приложений часто встречаются системы, которые имеют последние обновления безопасности, но, тем не менее, доступ к ним оказывается возможным вследствие специфичных настроек безопасности или использования простых, и самое главное – при этом универсальных паролей.

Проводя анализ программных уязвимостях, нельзя не принимать во внимание то, что проблема выпуска обновлений – это проблема производителя, а проблема своевременной установки обновлений – это задача администратора. И решается она только правильной политикой установки обновлений, включающей в себя различные аспекты: тестирование, согласование с руководством, возможность отката и др. Архитектурные уязвимости также могут

возникать при разработке (например, атака SMB relay в Windows), так и при администрировании. К примеру, неправильное расположение компонент ERP на сетевом уровне, позволяет получить неавторизированный доступ в подсеть ERP и, как следствие, осуществить перехват данных.

Подзадача 2. Бизнес-приложение является внутренним приложением – отсутствие проблем из сети Интернет

Взгляд с точки зрения руководства

Возникновение второй задачи часто относится к внутренним корпоративным системам класса ERP. Часто руководство организации допускает ошибку, суть которой заключается в том, что если к ERP-системе не осуществляется доступ из сети Интернет, то она считается безопасной относительно возможных действий внешнего злоумышленника. Эта ошибка является тривиальной, т.к. руководство организации в своей деятельности давно выходит за рамки внутренней среды. Множеству приложений приходится постоянно интегрироваться как с удалѐнными офисами через общедоступные сети, так и с другими компаниями посредством различных приложений по взаимоотношению с поставщиками, клиентами и партнѐрами, расположенными в разных частях мира. В то же время они также должны иметь постоянный доступ к ресурсам компании – это очевидное требование эпохи глобализации современного бизнеса.

В результате, сегодня все разработчики систем класса ERP предоставляют доступ к ERP-системе из сети Интернет. Примером этого может послужить платформа SAP ECC, в которой бизнес-процессы представлены как сервисы. Последствия этого шага с точки зрения безопасности вполне очевидны.

Но даже если ИС не имеет связей с внешним миром, остается общеизвестный факт – самым простым способом проникать в корпоративную сеть при использовании человеческого фактора (отправка пользователю письма с целью заманить его на злонамеренный сайт для последующей установки у него троянской программы). Однако при этом руководство организации часто полагает, что подобная атака предназначена только для проникновения в компьютерную ИС и не имеет отношения к ERP-системам. Это предположение является очень опасным заблуждением. Сегодня существуют специально разработанные сценарии таких атак, напрямую направленных, например, на SAP ERP, основанные на использовании уязвимостей SAP и методов социальной инженерии. Руководство организации должен отдавать себе отчет об уровне этой угрозы.

Взгляд с технической точки зрения

Злоумышленники уже давно не пытаются проникнуть в сеть компании напрямую через пограничные маршрутизаторы. Проще атаковать пользователей, которые наименее защищены.

На данный момент существует множество способов, позволяющих получить доступ к ERP-системе, находящейся внутри предприятия. Они основаны на различных уязвимостях клиентских приложений.

В ходе анализа защищенности клиентских компонент бизнес-приложений различных производителей, таких как SAP, Oracle и других менее известных, были обнаружены уязвимости, позволяющие получить доступ к компьютерам сотрудников через сеть Интернет. Кроме того, не стоит забывать о различных схемах социальной инженерии, также позволяющих получить доступ в корпоративную систему компании.

Другой известный и распространенный способ проникновения во внутреннюю сеть компании – использование уязвимостей в публичных WEB-сервисах, которые предоставляются клиентам. Примерами таких приложений могут быть SRM- и CRM-системы.

Как и в других WEB-приложениях, в их реализациях также присутствуют уязвимости, позволяющие не только получить административный доступ к самой системе или к документам других поставщиков (если рассматривать систему SRM), но и проникнуть внутрь компании из сети Интернет.

Наибольшую опасность представляет то, что для реализации данной атаки не обязательно иметь легитимные права пользователя в системе.

Таким образом, это может сделать любой злоумышленник.

Подзадача 3. Бизнес-приложения мало изучены – отсутствуют уязвимости

Взгляд с точки зрения руководства

Бизнес-приложения часто располагаются внутри корпоративной сети и, следовательно, изучены меньше, чем общеизвестные и широко используемые ОС и базы данных. Руководство организации не решает эту подзадачу по очевидным причинам, поэтому решением этой подзадачи занимаются технические специалисты и разработчики. Практика показывает, что это логично с точки зрения руководства организации, так как в этом случае разработчики, считают, что их система является внутренней (подзадача 2), сложной и недоступной для изучения большинства хакеров, практически не обращают

внимания на вопросы обеспечения безопасности. Это верно с точки зрения руководства организации, потому что безопасность, с точки зрения разработчика, никак не влияет на продажи продукта и только увеличивает срок его разработки и конечную стоимость.

В результате получается простой бизнес-вывод, который подтверждается практикой исследовательского центра Digital Security Research Group (http://www.dsecrg.ru), специализирующегося именно на поиске уязвимостей в бизнес-приложениях. Результат состоит в том, что безопасность бизнес-приложений, по определению, на несколько порядков ниже, чем безопасность типовых ОС (Windows, UNIX).

Взгляд с технической точки зрения

В популярных продуктах, таких как операционные системы Windows, офисные пакеты, антивирусы, дистрибутивы которых доступны огромному количеству людей, ежемесячно находятся новые уязвимости. Также существует информация о специфичных настройках безопасности и возможностях их обхода. Несмотря на то, что в этих продуктах присутствует множество уязвимостей, они постепенно становятся более защищенными, во многом, благодаря независимым исследователям, которые анализируют безопасность систем, уведомляют разработчиков о найденных уязвимостях и пишут на основе своих исследований различные аналитические статьи.

При использовании бизнес-приложений возникает прямо противоположная ситуация, когда большинство систем являются закрытыми, а проверкой их безопасности, занимается производитель (что само по себе – редкость, особенно для российских компаний-разработчиков) или квалифицированный администратор. Все это приводит к некоторой защищенности, так как злоумышленник не знает, как именно работают эти “закрытые системы” и, соответственно, не знает, как получить к ним неправомерный доступ.

Но это ошибочно, так как подход “Security through obscurity” (безопасность, основанная на скрытии механизмов защиты) не верен. Многолетняя практика центра Digital Security Research Group наглядно подтвердила то, что за время выполнения работ по анализу защищѐнности различных бизнес-приложений (работающих в банковской, в топливно-энергетической, в ритейл-сферах) находится множество тривиальных и особо опасных уязвимостей в архитектуре безопасности. Подобные уязвимости редко встречаются в публично доступных системах, которые постоянно подвергаются всестороннему анализу специалистов по безопасности и хакеров.

Подзадача 4. Безопасность ERP-систем – это матрица SOD, которая устраняет проблемы с безопасностью

Взгляд с точки зрения руководства

Наиболее типовой и опасной по результатам применения является подзадача, суть которой состоит в том, что между понятием безопасности ERP и наличием продуманной матрицы SOD ставится знак тождественного равенства. То есть, руководство организации считает, что для обеспечения безопасности ERP-системы достаточно пригласить консультанта, который разработает и внедрит матрицу SOD, и таким образом вся ERP-система станет безопасной. Руководству организации такое заблуждение простительно, техническим специалистам – нет.

Для руководства организации можно привести аналогию – установка правильных прав пользователей на контроллере домена не является бесспорным фактом того, что ИС в целом безопасна. Для ERP-систем это также применимо.

Руководство организации должно понимать, что матрица SOD – один из многих важных элементов обеспечения безопасности ERP-системы в целом.

В противном случае, ERP-система с матрицей SOD будет напоминать "дорогие стальные ворота с дорогой современной системой контроля доступа и видеонаблюдения".

Взгляд с технической точки зрения

Говоря об уязвимостях бизнес-приложений, необходимо рассматривать различные уровни, на которых это приложение работает. К таким уровням относятся:

- Сетевой уровень.
- Уровень операционной системы.
- Уровень СУБД.
- Уровень самого бизнес-приложения или ERP-системы.
- Уровень дополнительных компонентов и Web-приложений.
- Уровень клиентских компонентов ERP-системы.

Недостатки на одном из уровней могут привести к полной компрометации системы даже в случае идеально настроенной матрицы SOD. На сетевом уровне уязвимостью может являться отсутствие шифрования данных при передаче, на уровне ОС – отсутствие последних обновлений безопасности, на уровне СУБД – стандартные пароли и прочее. Таким образом, рассматривая безопасность бизнес-приложений, необходимо рассматривать систему в комплексе.

Заключение

В целом, необходимо отметить основную глобальную проблему, связанную с безопасностью бизнес-приложений: тотальное недооценивание производителями и потребителями вопросов, связанных с информационной безопасностью. При этом именно бизнес-приложения являются основой всего бизнеса компании. Возникает два парадокса: эта основа является априори абсолютно небезопасной, требующей к себе самого пристального внимания, этой основе не всегда уделяют достаточно внимания. С практической точки зрения центра Digital Security Research Group, на следующем витке эволюции средств обеспечения информационной безопасности основное внимание будет уделено вопросам безопасности бизнес-приложений, которые под давлением руководства организаций сейчас начинают выходить на первый план.

Поступила в редколлегию 31.03.2010

Рецензент: д-р техн. наук, проф. С.В. Листровой, Украинская государственная академия железнодорожного транспорта, Харьков.

АНАЛІЗ БЕЗПЕКИ БІЗНЕС-ДОДАТКІВ

І.Д. Медведовський, О.М. Поляков

Розглянуто забезпечення безпеки корпоративних бізнес-додатків як одне з найважливіших завдань сучасного бізнесу. Проводиться декомпозиція поставленого завдання, розглядаються сфери застосування виявлених підзадач, їх достоїнства і недоліки.

Ключові слова: *безпека бізнес-додатків.*

ANALYSIS OF SAFETY OF BUSINESS-APPLICATIONS

I.D. Medvedovskiy, A.M. Polyakov

Providing of safety of corporate business-applications is considered as one of major tasks of modern business. Decomposition set the problem is conducted, purviews exposed subtask, their dignities and failings, are examined.

Keywords: *safety of business-applications.*