BIZ KV:A КОМПЬЮТЕРНЫЕ ВЕСТИ www.kv.by

No. 001 (6)
18 января 2013 года

ООО “РГ “Компьютерные Вести” • Тираж: 11283 экз. • Адрес: Минск, ул. Мельникайте, 2, оф. 710 • E-mail: info@kv.by • Тел. редакции (017) 203-90-10 • Размещение рекламы: adv@kv.by

ERP — что в имени твоём?

Эдуард ТРОШИН

Думаю, что далеко не все читатели нашего издания знакомы с ERP-системами. Зато этот термин хорошо известен опытным системным администраторам и программистам. Но простой пользователь компьютера, даже продвинутый, может и не знать, что это и с чем его едят.

Все мы отлично знаем, допустим, какие программы установлены на компьютере у бухгалтера нашего предприятия. Скорее всего, это Word, Excel, или их аналоги под Linux, 1С (система автоматизации бухгалтерского учёта с лицензией на одно рабочее место) и ещё что-нибудь. Зачем ещё что-то, спросите вы?

Ответ очень прост — ERP-системы нужны для упорядочения документооборота и сбалансированного управления предприятием. Согласитесь, что в большой компании, которая работает с документами обычных форматов, несложно будет заблудиться в различных отчётах, справках, балансах. Можно что-то напутать и даже сделать это не единожды. Причём, путаться могут представители различных отделов, да ещё и в разных городах. Люди могут многократно вносить правки в один и тот же документ, не предупреждая об этом тех, кто его создал.

Такая работа может вызвать не просто беспорядок, а настоящий бардак. Именно поэтому внедрение ERP-системы является необходимым условием для всех публичных компаний с 1990 года.

Немного подробностей

Определение ERP в Википедии звучит достаточно сложно и громоздко, так что попробуем упростить эту формулировку по-своему. На нижнем уровне ERP-система работает так, что каждый документ, создаваемый, к примеру, в любом из финансовых отделов компании, отражается и на всех остальных финансовых отчётах. Там автоматически меняются необходимые цифры, подправляются графики, выполняются необходимые дополнительные расчёты. Итоговая информация поступает в смежные отделы и изменяет данные, которые имеют отношение к финансам. Таким образом, вновь заполненный или изменённый документ создаёт своеобразную “информационную “волну”, которая изменяет данные во всех, остальных, связанных с ним в системе.

ERP состоит из многих модулей, которые обеспечивают бизнес-процессы в различных подразделениях. Это, например, модуль электронного документооборота, модуль CRM (система работы с клиентами), веб-модуль, внутренняя служебная почта и система сообщений, модуль веб-телефонии и т.д.

Каждый сотрудник любого подразделения имеет доступ (при необходимости и через смартфон) к необходимой ему информации в общей ERP-системе. Правда, только в пределах своей компетенции. Если ему потребуются иные данные, то надо будет запрашивать их официально, через начальство.

Естественно, реализована в ERP и возможность одновременной работы с документами в многопользовательском режиме (почти как в Google и Википедии). Ведь если вы, одновременно с другим сотрудником компании, вызовете по локальной сети один и тот же документ Word, то для того, кто сделает это позже, возможность правки будет заблокирована. В ERP всё будет работать, а все правки и вся информация о них будут отражены в отдельном файле или списке. Естественно, любой документ сразу же можно будет “откатить” до

ERP — что в имени твоём?

любого предыдущего этапа исправлений.

Для руководства крупных компаний ERP-система просто необходима. Руководитель или акционер предприятия, используя её возможности, может получить исчерпывающую информацию о его работе и работе каждого подразделения, причём в любой удобной ему форме — в виде отчётов, графиков или текстовых данных за любой период времени. Более того, в некоторых случаях ERP-система может помочь и в выборе правильного решения или стратегии управления.

Ложка дёгтя

Главная проблема, которая тормозит внедрение ERP-систем у нас — это их стоимость. Речь идёт не только цене продукта, но и о его адаптации, внедрении, сопровождении. Цена лицензии ERP-системы одной известной западной компании для одного рабочего места стартует от 7 тыс. долларов. Стоимость внедрения на одно рабочее место может быть почти такой же. В итоге, внедрение ERP на крупном предприятии (скажем, на “АвтоВАЗе”) выливается в миллионы долларов. Вследствие дороговизны многие компании пытаются создавать какие-то системы сами, иногда неплохие, а порой — совсем неважнецкие.

Есть, конечно, системы и значительно дешевле, например те, что созданы у нас (лицензия на одно рабочее место обойдётся от 1 до 2 тыс. долларов). А те, что сделаны на основе пакета 1С:Предприятие, будут и вовсе недорогими (от 150 долларов за место). Но и функционал таких систем может оказаться недостаточным или неполным. Вдобавок они, как правило, не предназначены для одновременной работы с большим количеством пользователей.

Человеческий фактор

Но это далеко не все проблемы, связанные с внедрением ERP. Нужно ведь ещё адаптировать систему и сделать это правильно (чтобы она облегчила и ускорила работу). Для этого компетентные специалисты со стороны заказчика и компании, которая избрана для внедрения проекта, должны проработать все нюансы будущей системы.

На внедрение ERP в серьёзной компании требуется несколько лет. Необходимо изменять многие бизнес-процессы, а для этого требуется жёсткое решение руководства. К примеру, я слышал, как начальник ВЦ одного крупного белорусского предприятия жаловался, что бухгалтера отказываются работать с ERP. Ведь для того, чтобы исправить ошибку в отчёте, до внедрения системы им надо было всего лишь поменять цифры в одном-единственном документе и распечатать его заново. А с новым комплексом потребовалось “откатывать” и всю связанную с отчётом документацию фирмы. А это, естественно, вызывало скандал.

Проблем на этапе внедрения ERP всегда очень много и поэтому, до недавних пор бытовало мнение, что свыше 90% всех установленных ERP-систем не оправдывают ожиданий, работают недостаточно эффективно, а то и вовсе тормозят деятельность предприятий. Но уйти от них не получается. Рано или поздно, они появятся везде — такова современная реальность. Наличие ERP-системы от ведущих мировых разработчиков повышает даже стоимость акций компании.

ERP с открытым кодом

Существует целый ряд ERP-систем с открытым кодом. Например, популярный комплекс с незамысловатым названием OpenERP, а также другие — ADempiere, Compiere, Openbravo, Opentaps, xTuple. Все они созданы на западе, где ERP-системы чрезвычайно дороги, но необходимость в них гораздо серьёзнее, чем у нас.

Естественно, эти комплексы не обладают всем необходимым набором модулей, местами недоработаны и даже не русифицированы. Правда, некоторые из них всё же имеют платные версии, с расширенным функционалом и технической поддержкой.

Стоит сказать, что ERP— сложный программный комплекс, совершенствование и доработка которого требует немалых человеческих ресурсов и времени. Поэтому, внедрение ERP-систем с открытым кодом — рискованная задача со многими неизвестными.

Тем не менее, хорошо, такие проекты, возможно, кому-то пригодятся и помогут. Например, молодой компании-стартапу, которая пробует пробиться на рынок готового программного обеспечения и не знает, с чего начать. Вот такой вот намёк...

Обсудить

Глава Oracle СНГ:

“Мы смотрим с оптимизмом на возможности развития белорусского рынка”

Беседовал Вадим СТАНКЕВИЧ

Пользуясь присутствием вице-президента Oracle, главы представительства Oracle СНГ Валерия Лановенко, в Минске, “Компьютерные вести” решили поговорить с ним о работе Oracle в Беларуси, и не только о ней.

— Насколько белорусам интересны решения Oracle?

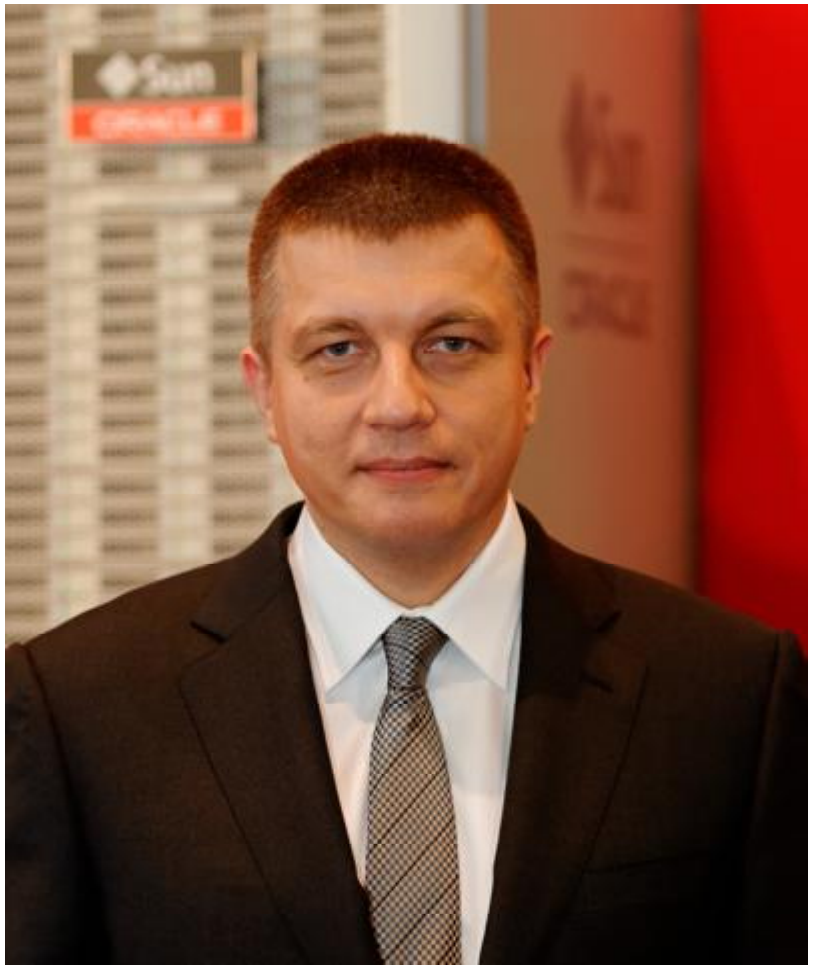
— В Беларуси достаточно высок интерес к инновационным решениям от Oracle. И подтверждением этому уже является количество слушателей, которые пришли к нам на форум к девяти утра.

— Какова сегодня стратегия Oracle в СНГ, какие решения компании наиболее популярны на постсоветском пространстве?

— Мы концентрируемся на предоставлении полного пакета услуг нашим клиентам, поскольку это заметно упрощает интеграцию. Что касается наиболее популярного продукта, то исторические реалии таковы, что Oracle — это компания, являющаяся лидером на рынке СУБД. Соответственно, именно этот продукт сегодня является номером один по количеству клиентов. Если же говорить о темпах роста их числа, то здесь уже лидируют другие продукты.

— А какие продукты компании сегодня наиболее интересны белорусскому бизнесу?

— В Беларуси у нас сегодня достаточно много как уже завершенных внедрений, так и пилотных проектов. Помимо СУБД, популярны сегодня такие продукты, как ERP-системы, CRM, а также многие другие корпоративные решения. К примеру, сегодня очень высок интерес к HR — системе для “управления талантами”. Она позволяет систематизировать обучение сотрудников, оценивать их работу, проводить профессиональный подбор кадров. Помимо этого, в последние годы возросло число внедрений связующего ПО (middleware) для интеграции бизнес-систем и бизнес-анализа. Кроме того, сегодня Oracle является игроком номер один в Беларуси в сегменте оптимизированных программно-аппаратных комплексов Oracle Engineered Systems — фактически, именно мы создали этот рынок, и видим в нем большой потенциал. Это такие комплексы как Exadata, Exalogic, Exalitics, SPARC SuperCluster и другие.



— Каковы, на ваш взгляд, перспективы развития Cloud-технологий в Беларуси?

— Думаю, что, как и во всём мире, перспективы эти очень хорошие. Облачные технологии будут стремительно развиваться, и тот, кто задумается об их использовании раньше конкурентов, окажется, соответственно, в более выигрышном положении. Тот же, кто будет упорно отказываться от их использования, может оказаться далеко позади.

— Как влияют изменения в белорусской экономике на бизнес Oracle в Беларуси?

— Во время кризиса предприятия ищут возможности оптимизировать свои расходы, для чего необходимы инвестиции в ИТ. Поэтому партнерская сеть не только не уменьшилась, но даже ещё и расширилась. Сегодня у нас на территории Беларуси работают более десяти специализированных партнеров, это примерно четверть всей партнерской сети

Глава Oracle СНГ:

“Мы смотрим с оптимизмом на возможности развития белорусского рынка”

и это довольно серьезная цифра, учитывая наши требования: партнеры должны обучать своих специалистов, иметь не менее двух проектов с положительными референсами, иметь ресурсы делать пилотные проекты, располагать возможностями по демонстрации аппаратных комплексов и решений. За два последних года наш офис Oracle в Беларуси вырос по численности более чем в 2 раза.

— Испытывает ли сегодня Oracle сильную конкуренцию в СНГ и, в частности, в Беларуси, со стороны других крупных международных игроков и местных компаний?

— Мы считаем, что конкуренция — это хорошо, потому что она не позволяет нам оставаться на месте и заставляет продолжать развиваться, причем активно. Сегодня Oracle является лидером в 72 продуктовых и отраслевых сегментах, среди них СУБД, Связующее ПО, CRM-системы, HR-системы, BI и EPM, UNIX-серверы, а также банковская и телеком отрасли, госсектор, образование, розничная торговля и многие другие. И, что особенно важно, по динамике у нас сегодня лидирующие позиции, потому что и в случае enterprise-решений для крупных предприятий, и в решениях для среднего бизнеса, мы, в отличие от других вендоров, ориентируемся на комплексное удовлетворение потребностей предприятий и предлагаем полный интегрированный стек продуктов. Я уверен, что Oracle еще более укрепит лидерство, когда предприятия “распробуют” облачные технологии, и их поддержка станет одним из определяющих факторов при выборе решения.

— Чем сегодня занят российский центр разработки Oracle? Нет ли планов открыть подобный центр в Беларуси?

— Этот центр разработки Oracle является одним из крупнейших в регионе EMEA. Он присоединился к Oracle вместе с приобретением компании Sun. В нем разрабатывают, в основном, Java, а также Middleware, Solaris, MySQL. В Беларуси у нас также трудятся несколько разработчиков, которые работают удалённо в виртуальных командах. Мы будем продолжать нанимать найденные здесь таланты, не оттягивая их в Санкт-Петербург или в другие центры разработки. Особая ценность местных разработчиков состоит в том, что они развивают локальное технологическое сообщество Oracle.

— А что нужно, чтобы попасть на работу в Oracle?

— Требования у нас, в целом, стандартные, но важно знание английского языка. Это совершенно необходимо, чтобы эффективно работать в виртуальной команде, собранной со всего мира. Oracle — это инновационная компания, нацеленная именно на разработку продуктов, поэтому мы ищем тех, кто, можно сказать, “горит” технологиями.

— Сталкивается ли Oracle с проблемами пиратства?

— Мы работаем в сфере B2B, и зачастую от правильного функционирования продуктов Oracle зависит работа всего предприятия. Это последнее, на чём экономят. Если вдруг произойдет сбой в системе, и у предприятия нет доступа к технической поддержке, то это ЧП. Поэтому наша задача состоит не в борьбе с пиратством, а в помощи клиентам в выборе оптимальной для них модели сотрудничества с Oracle.

Обсудить

Создание отдела информационной безопасности

Владимир БЕЗМАЛЫЙ, специалист по обеспечению безопасности, MVP Consumer Security, Microsoft Security, Trusted Advisor

Практический опыт показывает, что для результативного и эффективного решения проблем информационной безопасности необходимо создавать соответствующее самостоятельное подразделение. Попытки решить проблему иным способом позволяют в лучшем случае добиться успеха частично. Вместе с тем стоит помнить, что не бизнес существует ради безопасности, а безопасность существует ради бизнеса.

В наше время трудно кого-либо удивить происшествиями в области информационной безопасности. Все чаще мы сталкиваемся с различными угрозами в этой области. Практически каждый день приносит все новые и новые сведения об атаках хакеров (заметим, только что обнаруженных и нередко успешных), вирусных эпидемиях, атаках со стороны обиженных сотрудников. Именно последние становятся наибольшей угрозой в различных организациях.

Картина вырисовывается безрадостная, а выход состоит в создании хорошо подготовленного подразделения — службы защиты информации, или, как ее еще называют, службы компьютерной безопасности.

Казалось бы, можно возложить эти задачи на системного администратора или в крайнем случае создать отдельную единицу — администратора информационной безопасности в составе ИТ-подразделений.

Допустим, вы решили выбрать один из этих двух вариантов. Давайте рассмотрим, к чему же это приведет.

В первом случае системный администратор, фыркнув про себя, повернется и уйдет, думая, что он и так занимается вопросами информационной безопасности. Но у него и без того масса работы, а следовательно, либо задачи по защите информации будут выполняться в последнюю очередь, либо качество остальной работы заведомо ухудшится. Кроме того, системный администратор, в силу своего подхода к решению подобных задач, постарается решить ее исключительно техническими методами. И это приведет к тому, что задача решена не будет, так как информационная безопасность — это комплекс организационно-технических мер, и одних лишь технических методов решения здесь недостаточно.

Второй вариант лучше предыдущего, но не намного. В этом случае финансирование защиты информации будет осуществляться по остаточному принципу. Будет ли руководство фирмы прислушиваться к мнению какого-то там администратора информационной безопасности? Тем более если мнение последнего будет противоречить мнению начальника службы ИТ? А ведь любое предположение администратора информационной безопасности будет “портить жизнь” персоналу ИТ-службы. Как вы думаете, долго ли начальник ИТ-службы будет терпеть самостоятельного администратора информационной безопасности?

Служба информационной безопасности должна быть самостоятельным подразделением и подчиняться напрямую первому лицу в организации.

“Люди, ведающие воротами, оружием и охраной, зачастую действуют автономно от сотрудников, занимающихся ИТ, — комментирует Крис Кристиансен, аналитик IDC. — Необходимо, однако, иметь информацию о том, кто был в здании, куда пошел, к каким информационным системам мог получить доступ. Две службы, отвечающие за безопасность, должны работать скоординированно, и тогда каждая из них станет сильнее”. Наверное, в будущем мы увидим объединение служб физической и информационной безопасности, однако, на мой взгляд, это эволюционный процесс и на данном этапе еще довольно сложно найти людей, которые были бы специалистами в обоих вопросах.

В большинстве случаев специалисты в области информационной безопасности ничего не понимают в безопасности физической, и наоборот, поэтому насильственное слияние двух подразделений будет только мешать работе. Печальные свидетельства тому имеются в изобилии. При подчинении одной службы другой на подчиненной будут просто экономить. Зачем оплачивать то, чего не понимаешь! Мой практический опыт показал, что на данном этапе эти службы должны работать в тесном сотрудничестве, но не быть во взаимном подчинении.

Вместе с тем стоит помнить, что не бизнес существует ради безопасности, а безопасность существует ради бизнеса! На предприятии должна быть создана устойчивая “треугольная” структура — “аудит — служба защиты информации — ИТ-служба”. Необходимо четко определить границы ответственности, чтобы служба информационной безопасности не превратилась в неподвластного никому, контролирующего все монстра.

Как только речь заходит о средствах защиты информации, все сразу вспоминают межсетевые экраны и антивирусные программы, но это не панацея. Какое бы приложение вы ни купили, потребуется человек, который будет его обслуживать. Нет ничего хуже, чем великолепное антивирусное программное обеспечение,

Создание отдела информационной безопасности

которое содержит старые антивирусные базы. Руководство уверено, что антивирусная защита существует, но ввиду быстрого устаревания антивирусных баз его ценность равна нулю. То же касается и межсетевых экранов.

Нетрудно подсчитать, что содержание службы информационной безопасности из трех человек (минимальный состав отдела информационной безопасности — начальник, аналитик и администратор ИБ) обойдется компании намного дешевле возможных убытков. Следует смириться с тем, что данный отдел никогда не будет приносить явную прибыль, однако его назначение — уменьшить возможные убытки.

По сравнению с физической безопасностью, информационная находится еще на начальной стадии развития, образно говоря, в младенчестве. Она ориентирована на киберпространство, где все должно быть определено только при помощи нулей и единиц. Это приводит к непониманию со стороны руководства необходимости различных мер защиты. Чтобы обосновать приобретение соответствующих технических и программных средств, необходимо объяснить их назначение простым и понятным руководству языком.

Специалисты, где вы?

Существует два пути создания службы информационной безопасности. Первый — создание отдела информационной безопасности за счет подготовки, реорганизации и перераспределения ИТ-специалистов. Для отражения вирусной атаки можно привлечь собственных программистов, но в этом случае их основная работа окажется невыполненной. И неизвестно, что обойдется дешевле — набрать новый отдел или дергать своих сотрудников. “Хорошая безопасность означает предотвращение вирусов и атак, их своевременное обнаружение и немедленную реакцию на них. Если вы не создаете команду для обеспечения этого процесса, вы подвергаете свою компанию более высокому риску, связанному с последствиями внешних атак”, — говорит Девид Соул, исполнительный вице-директор и директор информационной службы страховой компании Zurich North America.

На практике трудно оценить урон, который может быть нанесен в результате хакерских атак. Можно оценить ущерб от вирусной атаки или от потери информации. Но как подсчитать ущерб, нанесенный репутации организации? Как правильно оценить ущерб от недополученной прибыли? Многие, и автор этой статьи в их числе, считают, что нельзя отвлекать ИТ-персонал от их прямых обязанностей для решения задач безопасности, потому что решение бизнес-задач отодвинет задачи обеспечения безопасности на задний план. Ведь основное дело компании — получать прибыль, а не обеспечить собственную безопасность.

Поиск талантливых профессионалов по безопасности может быть весьма трудным, а переподготовка имеющихся кадров в области ИТ и новичков в области безопасности — долгой и дорогостоящей. Возможен еще один вариант — привлечение внешних компаний для решения проблем безопасности. Но в этом случае вы должны будете избрать ту компанию, которой вы готовы доверить все свои секреты.

Менеджеры, ведущие поиск талантливых, опытных специалистов по безопасности, знают, что их не так много. Разрыв между спросом и предложением на таких специалистов очень велик.

Рекомендации по подбору персонала

— Вам нужно понять, для чего вы нанимаете специалиста. Ни один уважающий себя профессионал в области безопасности не захочет работать в компании, которая не понимает, для чего его нанимают.

— Будьте готовы к тому, что квалифицированная помощь стоит дорого.

— Индустрия безопасности — очень закрытая область, поэтому стоит заранее обратить внимание на специалистов из секретных служб, армии.

Университеты, которые имеют хорошие учебные программы с курсами по информационной безопасности, также могут предоставить начинающих специалистов.

— Можно искать специалистов в компаниях, предоставляющих услуги по безопасности.

Если вы по тем или иным причинам не желаете или не можете искать специалистов на стороне — обратите внимание на собственный персонал. Перед вами обязательно встанут вопросы отбора кандидатов и их обучения. Наиболее подходящие кандидаты — сетевые администраторы. Они обладают хорошими техническими знаниями и некоторым представлением о решении проблем безопасности. Кандидаты для переподготовки должны быть добровольцами. Нельзя заставить заниматься безопасностью “из-под палки”. При отборе кандидатов обращайте внимание на наличие навыков межличностного общения. Основное в работе сотрудника информационной безопасности — умение общаться с людьми. Эта работа связана не только и не столько с техникой и технологиями, сколько с умением говорить с людьми, заниматься организационными вопросами, писать документы и даже быть немного психологом! Кроме того, если человек занимается безопасностью, то он должен понимать, что на этой работе друзей у него нет! Ведь ему всегда нужно понимать, что предают только свои!

ИТ-специалисты и значительная часть ИТ-руководителей нередко воспринимают ИТ как привлекательную дорогую игрушку, которую хочется “потрогать”, изучить, проверить на прочность и т. п. Проблемы предприятия, в том числе проблемы информационной безопасности, этих людей волнуют в той степени, в какой позволяют приобретать эти самые игрушки за деньги предприятия.

Чтобы ИТ-инженеры стали специалистами по информационной безопасности, должны измениться акценты их сознания. Им следует не развлекаться с ИТ-игрушками, а защищать

Создание отдела информационной безопасности

предприятие. Вероятно, это самое сложное — научить людей мышлению охранников, защитников рубежей своего предприятия или организации. Это все равно что из разгильдяев мальчишек сделать солдат и офицеров — защитников Отечества.

Итак, вы набрали кандидатов в подразделение. Чему их следует учить?

В учебную программу должны входить:

— теоретические и методологические основы защиты информации;

— правовые основы защиты информации;

— основы криптографии;

— основы сетевой информационной безопасности;

— аудит информационной безопасности;

— создание организационных документов в области защиты информации (политика безопасности, правила при работе в Internet, правила работы с электронной почтой, политика аутентификации и пр.).

Вы скажете, что это слишком много. Можно обойтись лишь антивирусными программами, файерволами, системами обнаружения вторжений и т. д.

На самом деле, нет. Попробуем продемонстрировать это на примере использования электронной почты.

Предположим, ваш сотрудник систематически передает информацию конкурентам посредством электронной почты. Что вы можете сделать, если обнаружили это? Оказывается — ничего! Если вы начнете проверять его почту (организационных документов у вас в фирме нет, напомню), то сразу возникнет вопрос — что нарушил ваш сотрудник? Положение о коммерческой тайне? Так его нет. Положение о недопустимости отсылки подобных документов через Internet? А каких подобных? Кроме того, ведь вы сами нарушаете Конституцию, в частности ее главы о личной переписке. Пока не принят документ о том, что вся переписка принадлежит фирме, по закону она — личная! Итак, я надеюсь, вы поняли, что без юридически значимых документов вы не сможете привлечь к ответственности вашего сотрудника. Мало того, еще и вас могут привлечь к суду.

Предположим, что вы создали подразделение, нашли хороших работников, теперь вы должны их удержать. Инструменты, признание значимости и высокий уровень оплаты — вот основные факторы успеха.

Инструменты. Профессионалы, работающие в области информационной безопасности, стремятся стать профессионалами с большой буквы, асами своего дела, специалистами на вершине пирамиды. Использование самых новых инструментов и технологий позволит им чувствовать себя на передовых рубежах своей профессии. Если вы обладаете разнообразной информационной средой, не забудьте сказать им об этом. Среди самых желанных “игрушек” для специалистов по безопасности можно назвать Nessus, LAN Guard, XSpider (сканеры сетевой безопасности), Snort (инструментарий обнаружения атак), RAT (Router Analysis Tool, системный тестер маршрутизаторов).

Признание значимости. Для привлечения кандидатов в качестве дополнительных стимулов предложите им оплату переподготовки, сертификации и участия в конференциях. Несмотря на то что большинство экспертов в области информационной безопасности считают, что сертификация не столь необходима, как навыки и опыт, наличие сертификата по окончании курсов поднимает их престиж в глазах учащихся и заставляет относиться серьезнее к процессу обучения. Такие производители инструментов по безопасности, как Symantec, Cisco Systems и Check Point Software Technologies, представляют собственные курсы подготовки по своим продуктам. Но такие курсы стоят очень дорого. Специалисты по безопасности “расцветают” от признания заслуг. Они могут потерять интерес к работе, если не чувствуют поддержку руководства. Это, конечно, справедливо для любой категории работающих, но специалисты этого профиля имеют самый широкий доступ ко всем вашим секретам. Поэтому в спорах между сотрудниками ИТ и сотрудниками ИТ-безопасности необходимо находить золотую середину (безопасность не мешает бизнесу, бизнес не мешает безопасности). Однако следует помнить о разумной достаточности безопасности. Если ваши секреты стоят 10 тыс. долл., то неразумно покупать систему безопасности за 100 тыс. долл.

Высокий уровень оплаты. Это основной инструмент признания. Не забывайте, что зарплата специалиста по безопасности должна быть на высоком уровне.

Необходимо, чтобы ваши сотрудники регулярно отслеживали угрозы с помощью таких ресурсов, как www.security-lab.ru (Россия), www.bezpeka.com (Украина), www.bugtraq.ru (Россия) и многих-многих других.

Безусловно, ни одна из указанных мер вам не поможет, если ваши специалисты в области ИТ не понимают необходимости введения мер безопасности.

Вместе с тем хотелось бы предостеречь сотрудников отделов информационной безопасности от опасности “задрать нос” и мыслей о том, что их будут бояться из-за статуса, а значит, будут слушать и уважать. Решающую роль в обеспечении безопасности будет решать их реальный авторитет как специалистов в своей области, а не статус и тем более не страх! Для успеха необходимо полноценное взаимодействие со всеми сотрудниками фирмы. Реально информационной безопасностью на фирме занимаются все! Служба ИБ — только контролирует, обучает и управляет усилиями пользователей, от уборщицы до директора. Первой и главной задачей сотрудников службы является умение зарабатывать реальный авторитет не статусом, не словами, а делами.

Обсудить

Облачный антивирус: замена антивирусу, основанному на сигнатурах?

Raymond from Malaysia

Проведя несколько недель за тестированием облачного антивируса, я, наконец, могу дать ответ на собственный вопрос: способен ли облачный антивирус заменить традиционный антивирус?

Я уже говорил, что ВСЕ антивирусы замедляют работу компьютера, и это факт. В настоящее время количество вредоносного ПО растёт с невероятной скоростью, если сравнивать с ситуацией несколько лет назад, и то же самое происходит с файлом вирусных сигнатур (размер сигнатурных файлов некоторых антивирусов превышает несколько сотен мегабайт). Просто представьте себе перекрёстную проверку одного файла, который вы хотите просканировать с помощью базы данных, содержащей миллионы записей... Некоторые производители антивирусов, такие, как AVG и Norton, используют по-настоящему быстрые и эффективные методы сканирования, что позволяет максимально сократить время выполнения полной проверки файла. Однако если рассмотреть антивирус Dr. Web, процентное увеличение выполнения полного сканирования больше 2000% по сравнению с AVG 2011.

Так как в облачном антивирусе отсутствуют сигнатуры, он предположительно не замедлит работу компьютера. Я провёл сравнительный анализ Panda Cloud Antivirus Pro, Immunet Protect Plus, Prevx, Trend Micro Titanium, и если сравнивать результаты с AVG Antivirus 2011, в котором используется традиционный метод, AVG 2011 оказался значительно быстрее! Не поймите меня неправильно, облачные антивирусы лёгкие, но определённо не самые лёгкие. Вторым важным аспектом являлась скорость обнаружения. Если антивирусу не требуется наличие сигнатур на компьютере, значит, для того, чтобы узнать, заражён ли файл, и для последующей его перепроверки с антивирусными серверами, он должен использовать метод обнаружения, основанный на поведении. Логически, облачный антивирус не может перепроверять КАЖДЫЙ файл на вашем компьютере с помощью серверов, а то время сканирования может занять часы или дни...

Я протестировал Panda Cloud Antivirus Pro, Immunet Protect Plus, Prevx и Trend Micro Titanium на:

a) 27 довольно старых вирусов (большинство антивирусов уже распознают их как угрозы)

b) 3 полностью нераспознанных вредоносных программы (2 трояна и 1 бот) с расширениями AARC, PXR и RD

c) 1 популярное средство удаленного администрирования (RAT) с расширением BSN.

Panda Cloud Antivirus Pro

— Обнаружил все 27 вирусов

— Не смог обнаружить AARC, PXR и RB

— Обнаружил BSN и смог успешно удалить его даже с включенной защитой процесса.

Immunet Protect Plus

— Обнаружил 26 из 27 вирусов

— Не смог обнаружить AARC, PXR и RB

— Не смог обнаружить BSN

Prevx

— Обнаружил 20 из 27 вирусов

— Обнаружил AARC и PXR, но пропустил RB

— Обнаружил BSN

Trend Micro Titanium

— Обнаружил 23 из 27 вирусов

— Не смог обнаружить AARC, PXR и RB

— Не смог обнаружить BSN

Я не тестировал Comodo Cloud Scanner и Hitman Pro, так как они являются сканерами по мере надобности и не предоставляют постоянной защиты. Zemana AntiLogger может заблокировать как (b), так и (c). Ради интереса, мне захотелось узнать, такая ли скорость обнаружения у Panda Cloud Antivirus Pro, как у традиционного Panda Antivirus Pro 2011. Так что я установил Panda Antivirus Pro 2011 и получил совершенно такие же результаты, как и у Panda Cloud. Prevx довольно хорош для обнаружения троянов, но он пропускает полностью нераспознаваемого RB бота.

Сравним скорость обнаружения у антивируса Panda Cloud со скоростями обнаружения у AVG, Avira и Avast:

1. AVG Free 2011 и Panda Cloud Antivirus Pro имеют одинаковую скорость обнаружения.

2. Avira AntiVir Personal не смог обнаружить AARC и RB.

3. Avast Free 5.0 пропустил 2 вируса, не смог обнаружить AARC, PXR и RB.

Сейчас я посмею сказать, что Panda Cloud Antivirus Pro вполне может стать заменой традиционному сигнатурному антивирусу. Скорость обнаружения также хороша, как и у Avira, AVG и Avast, а также не потребляет большого количества системных ресурсов. Также Panda Cloud Antivirus Pro легко настраивается благодаря небольшому количеству понятных параметров.

Обсудить

КОМПЬЮТЕРНЫЕ ВЕСТИ

Издатель: ООО "РГ "Компьютерные Вести"

Адрес: Минск, ул. Мельникайте, 2, оф. 710.

Для писем: 220004, г.Минск, а/я 57.

Телефон/факс: (017) 203-90-10

E-mail: info@kv.by

Редакция может публиковать в порядке обсуждения материалы, отражающие точку зрения автора. За достоверность приведенной информации ответственность несут авторы.

Группа компаний "БелХард" приглашает на работу

В связи с ростом масштабов деятельности и открытием новых направлений требуются **специалисты высокой квалификации** в международные проекты на полную занятость:

- **Программисты прикладных систем** J2EE, C#, C++, Delphi, Python,
- **Web-программисты** ASP.NET, PHP, Ruby, Flash и Web-дизайнеры,
- **Программисты мобильных приложений** iOS, J2ME,
- **Руководители проектов, бизнес-аналитики** (разработка ТЗ для АСУП),
- **Системные интеграторы** (сисадмины со знанием Java),
- **Функциональные тестировщики, тест-разработчики**.

Наши ценности — это сильная команда, постоянное профессиональное совершенствование.

Предлагаемые нами условия: достойные вознаграждения, премии за достижения, широкие карьерные перспективы, соц. пакет с льготами от резидента ПВТ, эффективные процессы (ISO, CMMI) и современный инструментарий, разнообразие творческих задач, благоприятная атмосфера в команде.

С нами Вы сможете реализовать себя в актуальных, интересных проектах!

Специальное предложение студентам ИТ-специальностей со знанием английского языка:

- Проводим набор на стажировку с последующим трудоустройством, направления: SW Tester и SW Developer (PHP, Java, C#, IPhone),
- Гибкий график и сокращенная до 30 часов рабочая неделя,
- Стажеры могут быть направлены к нам на преддипломную и производственную практику,
- Наши сотрудники-выпускники вузов получают возможность оформиться на работу в качестве молодых специалистов (по распределению).

Подробная информация о вакансиях, об интенсивно растущих секторах корпорации, бланк резюме: **www.job.belhard.com**.

E-mail для резюме: job@belhard.com.