Корпоративные информационные системы и безопасность предприятия

интегрум

Информационно-аналитический обзор №398

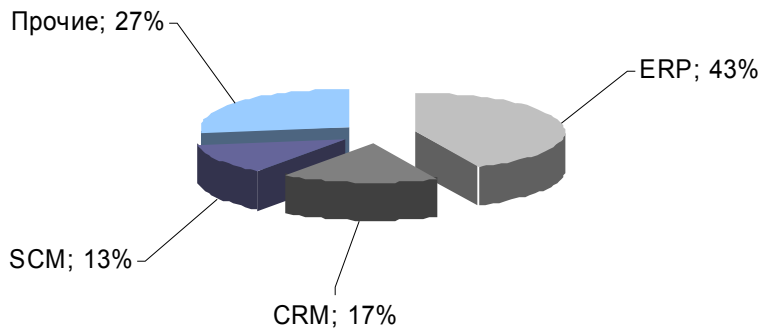
11 июнь 2010

Рынок

В условиях «информационного взрыва», характеризующегося накоплением гигантских объемов данных, конкурентным преимуществом становится способность не только извлечь из них нужную информацию, но и наиболее эффективно распределить ее между различными группами пользователей.

Одним из основополагающих принципов существования информационных технологий является их постоянное развитие. Модернизация технологий, методов и методик управления предприятием, вызванное постоянными изменениями ситуации на рынке, растущий уровень конкуренции, все это вынуждает руководителей компаний искать новые методы сохранения своего присутствия на рынке и удержания рентабельности своей деятельности: увеличивать мощности и производительности компьютерных систем, развивать сетевые технологий и системы передачи данных.

Диаграмма 1. Структура международного рынка корпоративных информационных систем



Безусловно, корпоративные информационные системы занимают важное место в бизнесе предприятий. В настоящее время выделяют следующие виды КИС: управления ресурсами предприятий (ERP); управления взаимоотношениями с заказчиками (CRM); управления цепью поставок (SCM) и ряд других, появившихся в последнее время (например, системы электронной коммерции и системы управления имуществом предприятий EAM (Enterprise asset management)).

В настоящее время на мировом рынке представлено более 500 КИС. На рынке ERP-систем, бесспорно лидируют компании SAP AG, Oracle, J.D. Edwards, PeopleSoft, Baan.

На сегодняшний день предприятия среднего бизнеса предпочитают зарубежные системы, но и отечественный производитель активно расширяет предложение. Российские системы достаточно широко разворачиваются на внутреннем рынке. В настоящий момент доля Российских корпоративных информационных систем приблизительно равна европейскому. Из года в год она растет приблизительно на 10%

Проблемы безопасности

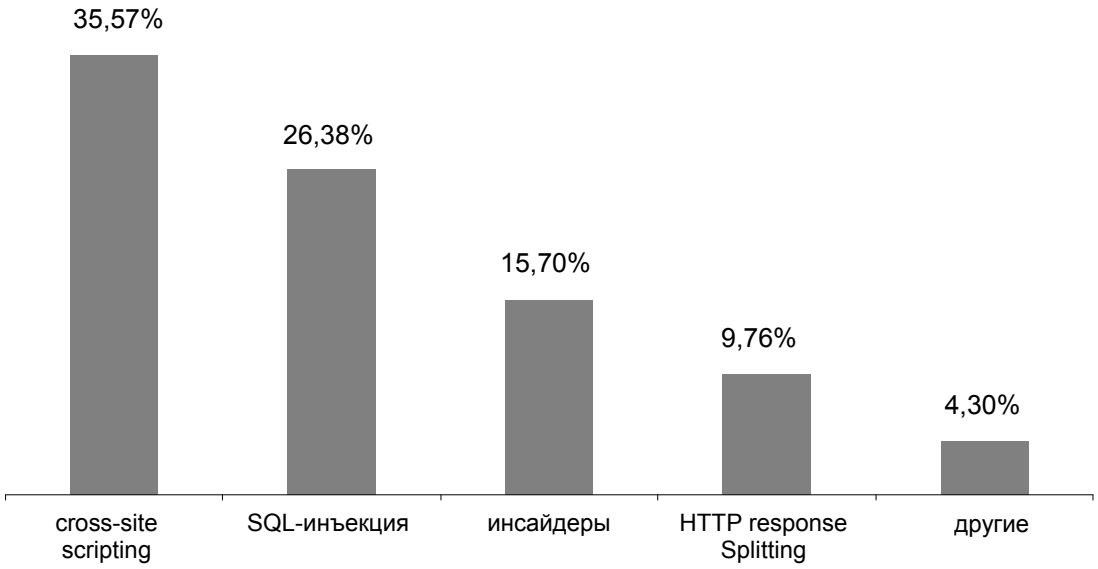
Появление новых информационных технологий и развитие компьютерных систем хранения и обработки данных привело к росту требований в части обеспечения безопасности. В настоящее время эффективность защиты информации растет вместе со сложностью архитектуры профильных систем.

Данные, хранящиеся в информационных системах компаний, являются объектом потенциального интереса злоумышленников. Будь то конкурирующие компании, или физические лица, которые могут извлечь выгоду, завладев и продав незаконно добытую информацию.

Техническая оснащенность систем безопасности в корпорациях растет, а уровень безопасности падает. И при этом хакеры кардинально не совершенствуют инструменты своих атак. Среди причин такой парадоксальной ситуации — снижение компьютерной грамотности, «взросление» хакерского бизнеса и недостатки технической защиты от атак. По статистике, к наиболее часто используемым атакам можно отнести несанкционированный доступ к паролю и конфиденциальной информации, несанкционированное удаленное выполнение команд вследствие ошибок типа “переполнение буфера”, нарушение прав доступа, атаки типа “отказ в обслуживании” и загрузка враждебного содержания (программ типа “троянский конь”, мобильного кода Java и ActiveX, вирусов).

Атаки производятся различными методами и каждый по-своему эффективен. Ниже приведена статистика атак на информационные системы.

Диаграмма 2. Статистика атак на информационные системы



Cross Site Scripting (XSS) — межсайтовый скриптинг. Возникает, когда в генерируемые сервером страницы по какой-то причине попадают пользовательские скрипты. Специфика подобных атак заключается в том, что вместо непосредственной атаки сервера они используют уязвимый сервер в качестве средства атаки на клиента (получения логина и пароля например).
SQL injection — внедрение SQL-кода. один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода. Атака типа внедрения SQL может быть возможна из-за некорректной обработки фильтрами входящих данных, используемых в SQL-запросах.
Инсайдеры — члены каких-либо групп людей, имеющей доступ к информации, недоступной широкой публике. Как правило, они производят физическую атаку защиты (кража носителя, нарушение доступности, целостности).
http response splitting — у язвимость являющаяся следствием того, что протокол HTTP позволяет прерывать заголовок и начинать новый, который и будет считаться "правильным" и обрабатываться "жертвой". Используя этот метод, злоумышленник может внедрить дополнительный HTTP-заголовок, который будет отключать фильтр XSS, и эксплуатировать уязвимость.

Примерами решений атак XSS служит постановка программных фильтров ввода информации например в поля форумов или личных сообщений. Фильтры анализируют информацию от клиента и, либо отсекают запрещенные знаки и пропускают информацию на сервер, либо запрещают отправку информации, выводя пользователю сообщение о вводе недопустимых символов. Такими символами могут быть: <, >, /, \.

Атаки типа SQL injection в целом похожи на вышеупомянутые. Основным их отличием является то, что скрипт вводится в поле запроса. Решением таких атак так же служит программный фильтр, анализирующий вводимые знаки. Для SQL-инъекций знаки почти те же: <, >, /, \,'.

Атаки инсайдеров решаются: тщательным подбором персонала, построением правильной корпоративной этики, разграничением прав доступа, контролем за перемещением документов и системой наказаний за нарушения.

http response splitting – относительно новый тип атаки на информационные системы,но получивший широкое распространение в хакерских кругах. Решением атак такого типа является специальные фильтры анализирующие запросы к web-серверу.

Свести к нулю риски, связанные с информационной безопасностью, невозможно. Можно лишь довести их до некоего управляемого приемлемого уровня, поэтому необходимо развивать не только технические средства защиты, но и организационные мероприятия.

Критерии выбора

Простейшую информационную систему можно построить на базе недорогих компьютерных комплектующих и доступного софта. Корпоративные информационные системы требуют иного подхода.

Комплексная система требует более скрупулезного подхода, как в выборе программных средств, так и в выборе оборудования. Основными производителями программно-аппаратных решений для корпоративных информационных систем являются такие фирмы как Cisco systems, IBM, SAP так и Российские производители как DEPO computers. Не маловажно то, производители комплексных систем, очень озабочены обеспечением безопасности своих продуктов. Они широко занимаются разработкой и внедрением программно-аппаратных средств по защите.

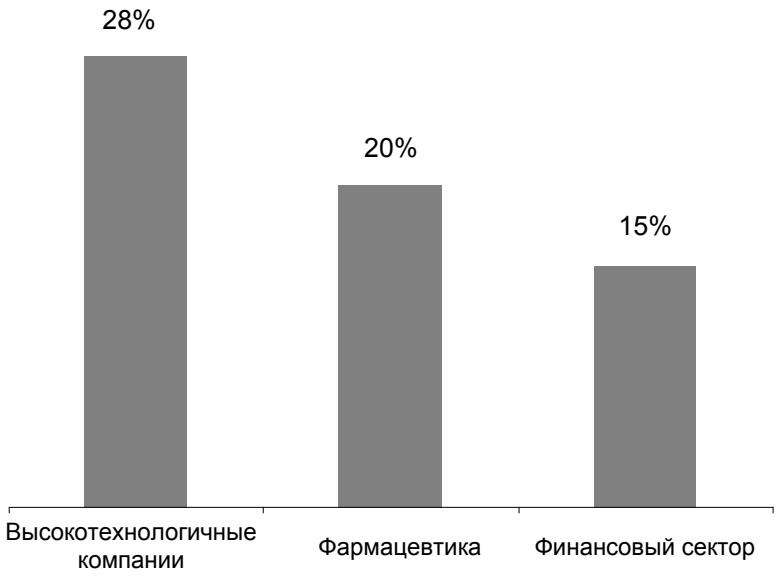
Так же не малым спросом пользуются и просто программные продукты специально разработанные для решения корпоративных задач: Baan, , Oracle Applications, «Галактика», «БОСС-Корпорация», в том числе систематизации, поиска и хранения информации: «Интегрум», ИАС «семантический архив».

Как показывают результаты исследований, по мнению поставщиков, основные критерии выбора КИС - это известность компании и функциональные возможности систем. Поставщики не рассматривают стоимость и требования к аппаратному обеспечению в качестве значимых факторов выбора.

При выборе корпоративной системы управления большого масштаба заказчики (обычно это крупные компании и холдинги) больше заинтересованы в эффективности оптимизации бизнес-функций и, как правило, готовы к большим затратам на лицензии и внедрение. Кроме того, сам факт внедрения корпоративной системы управления от крупного западного разработчика может увеличить рыночную стоимость и привлекательность предприятия для инвесторов.

Пользователи же считают основными параметрами при выборе российской КИС функциональные возможности, стоимость и гибкость системы. Наименее значимый фактор - требования к аппаратному обеспечению и масштабируемость.

Диаграмма 3. Отрасли-лидеры по затратам на КИС



Перспективы развития.

Российские КИС на данном этапе своего существования начинают создавать конкуренцию зарубежным, и поле для развития достаточно обширно. Интеграция информационных систем позволяет ускорить бизнес-процессы.

Корпоративные системы позволяют изменять, создавать, а порой и моделировать бизнес-процессы для выявления скрытых резервов предприятия и в конечном итоге повышения отдачи от производства. Удобные инструменты для этого во многом и определяют качество как самой эксплуатации и экономическую отдачу от внедрения корпоративной системы. И хотя сейчас крупные организации выбирают комплексные, зарекомендовавшие себя информационные системы, будущее у отечественных КИС есть, о чем говорит их ежегодный рост. Вероятно, что российские корпоративные информационные системы, в обозримом будущем смогут обозначить определенную конкуренцию производителям международного масштаба.

Сделано
в департаменте аналитики «Интегрум»

(495) 755-57-16

integrum.ru