Сколько должна стоить система обеспечения информационной безопасности на предприятии?

Все руководители задумываются о том, как защитить свой бизнес от тех или иных угроз. В настоящее время одной из самых серьезных опасностей для любой организации является угроза ее информационной защищенности. При том, что сегодня, пожалуй, уже не встретишь предприятия, которое бы совсем не заботилось о своей информационной безопасности, степень важности этой проблемы и риски для бизнеса, связанные с нарушением системы защиты информации, осознаются в полной мере далеко не всеми.

Чего хочет любой руководитель от системы информационной безопасности (ИБ) на своем предприятии? Очевидно, чтобы информация не пропадала безвозвратно, чтобы рабочие процессы протекали в непрерывном режиме, чтобы каждый сотрудник имел возможность получить нужную ему информацию и получить ее вовремя. При этом необходимо, чтобы определенные информационные ресурсы были доступны только тем лицам, которые имеют право с ними работать и, соответственно, чтобы к ним не имели доступа все остальные. Для того, чтобы обеспечить эти потребности, просто покупки системы безопасности недостаточно.

Что же еще требуется? Прежде всего, необходимо четко определиться, что мы должны защищать, от кого и почему мы должны это делать. Эти вопросы должны быть подробно прописаны в специальном документе – "Политика безопасности", который должен быть в обязательном порядке разработан в компании любого размера. Без отчетливого понимания целей защиты надежно защитить информацию невозможно.

Принятие решения о построении системы информационной безопасности и о размере бюджета, который будет выделен для этих целей, должно быть коллегиальным, поскольку объективно оценить эти вопросы один технический лидер компании зачастую бывает не в состоянии. К процессу разработки политики безопасности должны быть привлечены, помимо ведущих технических специалистов, бизнес-руководители и представители всех отделов, которые совместно должны решить, какие именно бизнес-процессы в организации нуждаются в защите. При этом необходимо помнить о важном постулате: вся система защищена настолько надежно, насколько защищено самое слабое ее звено.

Допустим, в компании достигнуто ясное понимание, что и от кого или от чего требуется защищать. Как же понять, сколько должно стоить внедрение системы по защите информации? При существовании на рынке дорогих и дешевых решений многие испытывают соблазн купить свою безопасность за меньшие средства или вообще обойтись бесплатными вариантами. Совершенно очевидно, что цена такой экономии может быть очень высока, превосходя во многих случаях стоимость самой дорогостоящей системы.

На сегодняшний день наиболее рациональный способ обоснования затрат в сфере информационных технологий основан на анализе ключевых показателей эффективности того или иного технического решения, таких как совокупная стоимость владения (TCO) и коэффициент возврата инвестиций в инфраструктуру предприятия (ROI).

При подсчете TCO необходимо учитывать, что в процессе эксплуатации возникают неявные или незапланированные затраты, которые зачастую превышают стоимость самой системы. По данным Gartner Group, прямые расходы на приобретение системы ИБ составляют только 15-21 % от общей суммы затрат на корпоративную информационную систему. Прямые затраты включают в себя такие "понятные" статьи расходов, как стоимость лицензии на антивирусные программы, системы предотвращения вторжений, затраты на аппаратное обеспечение (сервер или другую аппаратную платформу), затраты на изменение топологии сети, перенастройку ПО, а также стоимость внедрения, поддержки и обучения персонала, расходы на управление системой и зарплату администраторов.

Косвенные затраты плохо поддаются вычислению, поскольку связаны с работой системы в целом и имеют место в случаях простоев из-за сбоев или отказов каких-либо сервисов, что чаще всего бывает, когда пользователи еще не освоили в полной мере весь функционал системы и действуют методом "проб и ошибок".

При планировании бюджета на систему информационной безопасности надо учитывать еще один важный момент, а именно вопрос амортизации и износа активов. Не стоит забывать, что компьютеры и сетевое оборудование быстро устаревают и необходимо закладывать в бюджет средства на их модернизацию.

Кроме правильного решения вопросов бюджетирования, анализ и вычисление TCO нередко позволяет понять, что своими силами вы не можете справиться с эффективной эксплуатацией и поддержкой системы защиты, и вам стоит

подумать о передаче "опекунства" над вашей системой в "чужие" руки. Иными словами, расчет TCO позволяет во многих случаях обосновать необходимость аутсорсинга приобретенной системы обеспечения ИБ. И хотя для России такой вид услуг пока неактуален (много ли вы видели соотечественников, которые доверят чужому человеку "ключи от квартиры, где деньги лежат"), о нем стоит помнить.

Возврат инвестиций – ROI (Return Of Investment) – это отношение заработанных денег к тем, которые вкладываются, выраженное в процентах. Следует отметить, что универсальной формулы расчета для всех проектов не существует, и для каждого случая выводится своя формула. Общая формула подсчета ROI для проектов, связанных с внедрением систем ИБ, будет выглядеть так:

$$ROI = \frac{(Income + Risk + AddLosses)}{Investment},$$

где ***Income*** – показатель изменения доходов в результате внедрения системы информационной безопасности. Так как система ИБ непосредственно не используется для увеличения доходов компании, то, вероятнее всего, параметр "изменение доходов" будет равен нулю. ***Risk*** – это параметр, исчисляемый в денежном выражении и учитывающий не только предотвращенные потенциальные потери в результате действия той или иной угрозы, но и вероятность ее осуществления. ***AddLosses*** – предотвращенные потери, связанные с отсутствием системы ИБ, такие как снижение производительности работы администратора системы безопасности, потери времени на поиск информации об уязвимостях и атаках и т.п. ***Investment*** – инвестиции в систему ИБ. В общем случае это совокупная стоимость владения, описанная выше.

Итак, сделаем краткое резюме. Большую часть решений, связанную с реализацией разработанной политики безопасности, можно внедрять на уже существующей базе (разумеется, можно сделать и обоснованные инвестиции в сетевую инфраструктуру и телефонную связь). После подсчета показателя ROI (хотя бы приблизительного, с тем, чтобы понять, положительным он будет или отрицательным) можно корректировать бюджет или подход к реализации защиты и делать выбор либо в пользу аутсорсинга, либо принимать решение о привлечении тех или иных финансовых схем, например, таких как лизинг или кредитование.

На сегодняшний день комплексный подход к построению системы информационной безопасности организации предоставляет только компания Cisco Systems со своей концепцией Self-Defending Network, которая базируется на проактивных механизмах защиты и включает в себя решения по защите как рабочих станций и серверов, так и сетевой платформы и телефонии с единым центром анализа и управления. Так как все продукты компании содержат в себе полный функционал по безопасности, с их помощью в каждой организации можно создать эффективные механизмы по защите данных с минимальными капитальными затратами.

Например, если в компании локальная сеть построена на коммутаторах Cisco, можно, руководствуясь созданной на предприятии политикой безопасности, активировать те или иные функции, которые уже заложены в устройства (например, в линейке 2950 более 100 функций по безопасности), и если в сети есть маршрутизатор Cisco ISR (8xx,18xx,28xx,28xx) или старше, можно либо активировать функции файрвола, либо залить ПО, позволяющее реализовывать функции предотвращения вторжений. При этом необходимо продумать вопрос о нарастающей нагрузке на сетевые устройства и внедрять решения по безопасности, руководствуясь здравым смыслом. Чтобы обезопасить себя от риска принятия неправильных решений а свой бизнес от опасности ненужных потерь, во многих случаях целесообразно доверить разработку решения по ИБ опытному системному интегратору, который сможет определить оптимальный подход в каждом конкретном случае. И всегда по любым вопросам, касающимся информационной безопасности в организациях, можно обратиться в компанию Cisco Systems.

Андрей Повольнов, компания Cisco Systems

НОВОСТИ

Система управления ТОиР на базе EAM-системы iMaint

Компания "АНД Проджект" и ОАО "Рудас", специализирующееся на добыче, транспортировке, переработке и отгрузке высококачественного песка для строительных работ и образования новых намывных территорий, создали информационную систему управления техническим обслуживанием и ремонтами основных фондов и активов предприятия на базе EAM-системы iMaint.

Специфика предприятий добывающей промышленности заключается в том, что любые простои техники сразу же сказываются на прибыльности предприятия. ОАО "Рудас" использует технику западных производителей Volvo, Liebherr, и одним из "узких мест" на предприятии является оперативная доставка требуемых узлов и компонентов из-за рубежа. В рамках проекта было проведено детальное описание составных частей оборудования, объемов запасов и мест их хранения. Теперь справочная база предприятия полностью соответствует каталогам западных производителей техники, что позволяет быстрее доставлять необходимые компоненты для работы сотрудников ремонтных служб.

Продолжительность проекта внедрения EAM-системы iMaint составила 5 месяцев. На предприятии автоматизирована служба главного механика, отвечающая за эксплуатацию и модернизацию техники ОАО "Рудас". В январе система управления техническим обслуживанием и ремонтами (ТОиР) перешла в промышленную эксплуатацию.

Теперь специалисты отдела главного механика получают достоверную информацию о состоянии оборудования, автоматически формируют в системе графики ТО, отслеживают остатки запчастей на складах, в оперативном режиме формируют заказы на закупки в удобном для поставщиков виде. Сотрудники территориально распределенных цехов и ремонтных мастерских ОАО "Рудас" работают в системе iMaint в режиме "on-line" с помощью специального модуля iMaint Web.