Ключевые требования к средствам анализа и оптимизации рисков. «BCM-Analyser»

Методы анализа и оптимизации рисков, с точки зрения владельцев бизнес процессов, должны дать ответ на следующие простые вопросы:

- что нужно сделать, чтобы ущерб бизнес процессам от различных угроз был минимальным;
- сколько это будет стоить;
- какова величина остаточных рисков.

Чтобы ответить на эти вопросы постараемся сформировать самые важные требования к таким методам. При этом понятно, что любой метод, есть, по сути, отражение некоторой математической модели технологических процессов происходящих в конкретной системе и точен до определенной степени. Однако, учет ключевых факторов (все факторы априори учесть невозможно) должен позволить дать результат, погрешность которого будет минимальна.

Во-первых, такой метод анализа риска должен быть количественным, результат которого выражен в каких-либо денежных единицах – вряд ли удастся объяснить бизнесу разницу между качественными показателями, например, высоким уровнем риска и очень высоким.

Во-вторых, надо учесть все взаимосвязанные активы и свойства активов, так как задачи защиты от кражи оборудования с целью его продажи или кражи винчестера компьютера с целью использования конфиденциальной информацией могут решаться одинаково, например, установкой надежной входной двери. А если еще учесть, что помимо информации во многих организациях есть другие ценные ресурсы, то, теоретически, может оказаться, что более выгодно решать задачи регистрации доступа к компьютерам не с использованием паролей, а посредством установки систем видеонаблюдения за помещениями.

Определив активы и свойства, проанализируем, а все ли свойства одинаковы. Опыт подсказывает, что, как минимум, их можно разделить на два класса – свойства, нарушение которых приводит к нарушению состава и структуры актива (например, нарушение целостности оборудования) и которые не приводят (например, нарушение конфиденциальности информации). Если в первом случае для исправления ситуации необходимо восстановить актив, то во втором, достаточно прекратить процесс нарушения свойства. Соответственно, для разных свойств должны и отличаться подходы к их защите.

Далее, неплохо бы иметь в виду, что ущерб активу при проявлении угрозы, величина, изменяющаяся с течением времени. Ущерб бизнесу потенциально может расти не только с момента нарушения доступности актива, но и при реализации угроз, например, конфиденциальности информации, другим свойствам активов. Действительно, массив конфиденциальной информации не обязательно статичен (как какая-нибудь технологическая формула или секрет производства), потенциально он может изменяться с течением времени, вследствие, например, появления новой конфиденциальной информации или обесценивания старой. Соответственно, может существенно отличаться ущерб в случае разового несанкционированного доступа злоумышленника (например, к ноутбуку топ-менеджера) или если такой доступ будет постоянным в течение года.

Перейдем к контрмерам, которые обеспечивают защиту свойств активов от угроз. Так как анализ риска не самоцель, а лишь этап на пути определения оптимальных способов защиты от угроз, то метод должен в итоге давать не уровни рисков, а набор оптимальных решений по этим рискам.

Сформировать требования к контрмерам сложнее, поскольку они чрезвычайно разнообразны – это и организационные меры, технические меры, а также правовые, морально-этические, меры связанные со страхованием и т.п. Ситуация осложняется тем, что контрмеры даже одного назначения, отличаются в зависимости от производителя, т.е. нет, например, одинаковых по эффективности антивирусных средств. Исходя из этого, можно сделать первые выводы:

a) Метод должен учитывать все разнообразие контрмер, т.е. принципы описания и учета в анализе контрмер должны быть универсальными, подходящими для любых стратегий обработки риска (уменьшение, перенос, принятие или избежание). Механизм описания должен учитывать все важные свойства этих контрмер, т.е. процесс унификации не должен идти в ущерб их основной функциональности.
b) Метод должен позволять задавать одинаковые по назначению контрмеры разных производителей, так как нет одинаково хороших и одинаково плохих средств. Плюсы средств одного производителя в другой ситуации могут обернуться минусами. Например, бесплатное, но малоэффективное антивирусное средство, скорее всего, мало подойдет для защиты очень ценной информации и, наоборот, для малоценной информации вряд ли подойдет дорогой, но эффективный антивирус.

Пойдем далее, мало описать контрмеры, надо учесть, что они, как правило, связаны друг с другом, причем эти связи могут быть, весьма гибкими. Например, результат выполнения какой-либо одной функции многофункциональной контрмеры может использоваться уже совершенно другими контрмерами для реализации своих функций. Т.е. в методе должны задаваться связи между контрмерами, между различными функциями контрмер и эти связи должны учитываться при расчете рисков.

Вспомним, что вначале была поставлена цель получения стоимости оптимального способа защиты от угроз, и для этого сформулируем следующее требование как необходимость точного учета стоимости контрмер. А что такое стоимость контрмеры? Это, как минимум, единовременные затраты, постоянные затраты (затраты на обслуживание), а также затраты появляющиеся когда что-нибудь случилось (например, вызов специалиста по ремонту). При этом надо иметь в виду, что расчет полной стоимости надо производить не за год, а, хотя бы, за три, так как недорогая в установке контрмера может быть очень дорогой в обслуживании и, соответственно, наоборот, а это можно определить только на значительном интервале времени.

После того, как заданы десятки и сотни активов, а также их свойств, сотни или тысячи взаимосвязанных контрмер, метод должен предусматривать автоматический анализ всех возможных комбинаций контрмер с целью определения единственной, самой оптимальный комбинации. Ручной перебор, например, 1 млн. комбинаций (при всего-то 20 контрмерах) вряд ли кого-либо вдохновит на подвиги.

В заключение следует констатировать, что многие существующие средства анализа и оптимизации рисков не соответствуют данным требованиям и именно данные требования, а также практические навыки в построении систем безопасности легли в основу программного комплекса оптимизации рисков «BCM-Analyser».