Микроскопы не для гвоздей

Решения RSA: управление информационной безопасностью, менеджмент рисков, соответствие нормативам

Текст: Александр Иржавский, технический директор НТЦ «Вулкан»

Построение и внедрение политики информационной безопасности в финансовом учреждении – это не только организационные мероприятия, но и развертывание специализированных инструментов, помогающих персоналу в принятии решений и обеспечивающих поддержку деятельности специалистов по безопасности и управлению рисками. Подобные продукты относятся к категории hi-end решений, обладающих специфическим функционалом и ориентированных на заказчиков, достигших определенного уровня зрелости в ИТ и в управлении рисками. К таким системам относятся решения enVision и Archer eGRC Suite от компании RSA, The Security Division of EMC.

ЕСТЬ ЛИ ЛОГИКА В «ЛОГАХ»?

Любого ИТ-менеджера постоянно беспокоят фундаментальные вопросы: в порядке ли ИТ-инфраструктура, как дела с безопасностью, отвечаем ли мы всем требованиям? Ответы на эти вопросы содержатся в регистрационных журналах и в великом множестве генерируются оборудованием, системным ПО, приложениями, средствами защиты. Проблема заключается в большом объеме «логов» – людских ресурсов элементарно не хватает, чтобы обработать тысячи сообщений о событиях. В лучшем случае журналы накапливаются, но не обрабатываются, в худшем – не ведутся или уничтожаются.

Помочь в этой ситуации способна SIEM-платформа RSA enVision. Это решение обеспечит сбор (безагентный и высокопроизводительный), хранение (долгосрочное и в неизменном виде) и обработку (от простых отчетов до сложнейших корреляций) информации о событиях от любых объектов, разгрузит людей, позволит не упустить важный сигнал. А на случай серьезной проблемы – станет бесстрастным регистратором, свидетелем развития инцидента, ключом к выявлению виновных лиц и определению причин происшествия.

Пользователи enVision получают комплексное ИТ/ИБ-решение с высокой производительностью, отличной масштабируемостью, множеством функциональных возможностей, встроенным сервисом управления инцидентами и развитыми средствами визуализации информации. В активе enVision корреляционный анализ, гибкая отчетность (в том числе по линии соответствия PCI DSS), работа с экзотическими источниками, поддержка виртуальных сред и многое другое, что делает систему главным навигатором для ИТ-персонала в океане событий.

ВИЛЬГЕЛЬМ ТЕЛЛЬ КАК РИСК-МЕНЕДЖЕР

Самый запоминающийся эпизод в легенде о лучнике – выстрел Телля в яблоко, находящееся на голове его собственного сына. Риск – огромный, цена ошибки – жизнь. Но усилия Вильгельма Телля по снижению риска (годы тренировок) и правильная оценка обстановки позволили принять и успешно реализовать самое главное решение в его жизни. Может, поэтому профессия великого швейцарца стала названием уникального продукта для риск-менеджмента?

Решения, принимаемые руководством кредитно-финансового учреждения на основе анализа рисков, зачастую не менее судьбоносны для бизнеса и сотен тысяч бенефициаров – акционеров и клиентов. Только активов и факторов, на них влияющих, на несколько порядков больше. Сегодня банкам приходится иметь дело со множеством рисков, которые лежат в различных областях деятельности. Эти риски нуждаются в систематических мониторинге и оценке.

Будучи не в состоянии справиться с потоком рисковых событий, большинство банков управляет рисками фрагментарно, обращая внимание только на существенные риски и очень часто реагируя уже на реализовавшиеся рисковые события, что не позволяет развиваться и функционировать бизнесу в предсказуемом и запланированном темпе. Поэтому управление рисками – неотъемлемая часть и один из основных элементов корпоративного управления.

RSA Archer – система поддержки риск-менеджмента, которая позволяет одновременно управлять рисками во всех жизненно важных направлениях деятельности: операционными, финансовыми, рисками соответствия, ИТ-рисками.

Archer – это решение Enterprise-уровня в области Governance, Risk and Compliance. Модульный состав продукта позволяет создать комплексную среду для поддержки процессов управления рисками: от их идентификации до запуска контрольных процедур и распределения персонала, что позволяет вовлечь в процессы Risk Management весь персонал компании. Другими словами, применение Archer порождает новую культуру управления рисками.

КЛУБ С МИРОВЫМ ИМЕНЕМ

Решения RSA Security широко распространены на Западе, где к вопросам compliance и рисков традиционно относятся с уважением. В когорте передовиков капиталистического соревнования можно отыскать множество компаний с мировыми именами, использующих продукты RSA. Стабильный интерес к RSA enVision и практика успешных внедрений имеются и в России. А с 2011 года отмечается заинтересованность в платформе Archer, и символично, что основные потенциальные потребители этого решения сосредоточились в банковском секторе. А в самом деле – почему бы не перенять положительный опыт зарубежных коллег, создавая новые бизнес-ценности? NBJ