ARinteg делится опытом построения инфраструктуры и обеспечения информационной безопасности

Специалисты ARinteg совместно с экспертами компаний-партнеров Лаборатория Касперского, Arcserve, Huawei, Microsoft рассказали представителям финансовых, транспортных, промышленных компаний о лучших практиках построения защищенной и эффективной инфраструктуры современного предприятия, которые базируются на применении продуктов мировых вендоров программного и аппаратного обеспечения, а также на тесном взаимодействии служб информационной безопасности и информационных технологий.

Лучшие практики информационной безопасности

В Москве состоялся семинар компании ARinteg «Построение инфраструктуры предприятия и обеспечение информационной безопасности». Открывая дискуссию, технический директор компании ARinteg Сергей Трещалин отметил, что лучшие практики вырабатываются только в тесном взаимодействии служб информационной безопасности и информационных технологий компании. Такой подход позволяет получить синергетический эффект. «Это подтверждает опыт наших проектов с применением продуктов мировых вендоров программного и аппаратного обеспечения, с которыми компания установила прочное деловое партнерство, – говорит Сергей Трещалин. – Уже на этапе предпроектного аудита и консалтинга мы готовы предлагать лучшие рекомендации по созданию надежно защищенных корпоративных информационных сред».

Для ARinteg, специализирующейся на комплексных проектах в сфере информационной безопасности, безусловным вызовом времени является стремительная миграция бизнеса на мобильные платформы. Доступ в корпоративное информационное поле в режиме 24х7 из любой точки мира ранее порождал дополнительные риски и пользовательский дискомфорт. Теперь, по мнению выступившего на семинаре Сергея Нагорного из Microsoft, с использованием облачной платформы Microsoft Azure работа территориально распределенного предприятия, разъездного персонала не только безопасна с точки зрения сохранности коммерчески важной информации, но также удобна и высокопроизводительна.

Тем же компаниям, которые предпочитают иметь собственные вычислительные мощности, а также коммерческим ЦОДам, будут интересны решения компании Huawei. «Экосистема продуктов компании, – рассказывает Директор департамента ИТ-решений Huawei Артур Пярн, – простирается от серверных решений до носимых персональных устройств, включает системы хранения данных, системы виртуализации, мониторинга, сетевые подсистемы и прикладной софт. На технологиях Huawei можно создать территориально-распределенный ЦОД на базе нескольких физических ЦОД, а в случае необходимости легко выполнить перераспределение и перенос виртуальных мощностей».

При всей мощи и надежности аппаратных платформ от лучших вендоров бизнес не должен сбрасывать со счетов важность резервного копирования данных. Михаил Митрошин из недавно созданной на базе подразделения CA Technologies компании Arcserve рассказал о решениях, позволяющих обеспечить быстрое восстановление при сбоях, поддержать непрерывность бизнеса, гибко настроить процессы создания резервных копий в соответствии корпоративными регламентами.

Соблюдение регламентов также важно и в сфере управления информационными активами компании. Для многих организаций в силу отсутствия должного внутреннего контроля – это зона финансовых, репутационных и других рисков. 1 Марта 2015года международные стандарты (ISO/IEC 19770-1) дополнились вступлением в силу нового национального стандарта Российской Федерации – ГОСТ Р ИСО/МЭК 19770-1-2014. Олег Гончаров, продакт-менеджер ARinteg, представил новое предложение компании – оценку уровня зрелости процессов SAM (Software Asset Management, Управление программными активами), как первой стадии построения целостной системы управления ИТ-активами клиентов.

Применяя высокопроизводительные аппаратные платформы, компании получают возможность использования всех преимуществ виртуализации. Евгений Бударин из Лаборатории Касперского предупредил, что в погоне за быстродействием и снижением стоимости владения компании не должны забывать об особенностях защиты виртуальных сред. Эксперт рассказал о том, как соблюсти баланс между безопасностью и производительностью, применяя решение Kaspersky Security для виртуальных сред.

Для обнаружения инцидентов в сфере информационной безопасности, как правило, требуется обработка больших объемов данных, поиск информации и выявление различных видов корреляций. Специалист ARinteg Василий Коровицын продемонстрировал, как для эффективного решения данной задачи используется программный продукт Splunk. Инсталлировав Splunk с приложением Enterprise Security, пользователь получит классический Security Information and Event Management. Если же Splunk установить совместно с приложением PCI DSS, то пользователь получит полноценный центр по контролю за соблюдением требований PCI DSS.

Мошенники атакуют бизнес по всему спектру каналов и способов. Роман Семенов, Руководитель Отдела консалтинга и аудита ARinteg, на примере платежных банковских карт предствил обзор распространенных видов высокотехнологичного «отъема» денег и других активов у населения и компаний. Действенные и апробированные рецепты от ARinteg по противостоянию злоумышленникам включают построение комплексных систем защиты от утечек данных, установку видеонаблюдение в критичных зонах, средства защиты от DDoS атак, применение специализированных средств обнаружения и отражения нестандартных атак и многие другие решения, созданные с применением продуктов от мировых вендоров в ходе масштабных проектов.

Комментируя итоги мероприятия коммерческий Директор ARinteg Дмитрий Слободенюк отметил: «Для ИБ и ИТ специалистов предприятий семинары ARinteg открывают доступ ко всему арсеналу опробованных на практике решений и наработанной методологии ведения проектов компании. В свою очередь, ARinteg всегда готова делиться своим опытом!»