МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ВИРТУАЛЬНОЙ ИТ-ИНФРАСТРУКТУРЫ

К.э.н., доц. М.П.Чайковская

Одесский национальный университет имени И.И. Мечникова
Украина, г. Одесса
chmp@ukr.net

Современный этап развития технологий оптимизации ИТ-инфраструктуры предприятия характеризуется не только динамичными количественными показателями (большинство развертываемых сегодня серверов являются виртуальными, по прогнозам IDC, к 2013 году соотношение виртуальных серверов к физическим составит 2:3, а к 2014 году – 2:1) [1], но и качественно новыми тенденциями, связанными с переходом к новой эволюционной фазе внедрения технологий виртуализации на базе развертывания внутри компаний систем с высокой степенью виртуализации и автоматизированным управлением (построение “внутреннего” облака и организация его интеграции и взаимодействия с “внешними” облаками).

С одной стороны, это усиливает экономические преимущества виртуализации для предприятия: повышает эффективность использования ресурсов инфраструктуры; снижает затраты на физическую инфраструктуру и управление; облегчает управление и контроль над распределенной средой и доступом; повышает гибкость, управляемость, непрерывность ИТ-поддержки бизнеса, повышает скорость реакции на внешние турбулентности; снижает зависимость от оборудования за счет терминального доступа к десктопам, конвертированным в виртуальный вид; обеспечивает не только консолидацию приложений, но и управляемость ими по схеме соглашения об уровне обслуживания. Но с другой стороны, обостряются проблемы виртуализации связанные с вопросами безопасности и надежности облачных архитектур и средств их управления (более 60% развертываемых виртуальных машин в 2012 году оказались менее защищенными, чем физические), создается угроза для большого количества систем при

получении контроля над одной из виртуальных машин. Определенный эффект достигается при внутреннем реинжиниринге, связанным с выделением бизнес-процессов организации, которые не целесообразно виртуализировать (бизнес-процессы с экспоненциальным ростом трафика и высоким весовым коэффициентом сезонной компоненты, а также бизнес-приложения с высокой степенью специализации [2]).

Анализ модели угроз виртуальной инфраструктуры, позволил сформулировать требования к системе мониторинга и контроля для виртуальных сред; выделить критичные элементы системы и источники угроз: неинтегрированность информационных активов, наличие временно неактивных технических и технологических ИТ-ресурсов, незакрепленность на протяжении всего жизненного цикла системы профилей безопасности, слабый менеджмент персонала (человеческий фактор) и построить модель управления информационной безопасностью, включающую блоки, связанные с обеспечением целостности, сохранности и восстановления данных; защитой от несанкционированного доступа к данным; мониторинга и оценки выполнения требований стандартов безопасности и соответствия стандартам PCI DSS, CIS Networking; аудита на соответствие корпоративной политики безопасности.

Разработка модели информационной безопасности на этапе планирования ИТ-проекта позволит учесть его структурные и функциональные особенности, минимизировать издержки ресурсоемких операций, решить задачи аудита трафика, организации многофункциональных шлюзов и закрепления профилей безопасности, будет способствовать дальнейшему сокращению ИТ-издержек, увеличению гибкости системы и реализации конкурентных преимуществ.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Чайковская М.П. Перспективы развития технологий виртуализации в Украине// Аналіз сучасних економічних процесів та інформаційних систем// Матеріали Міжнародної науково практичної конференції. – Дніпропетровськ, 2011. - с.89-92.

2. Чайковская М.П. Инновационные технологии оптимизации ИТ-инфраструктуры предприятия// Економічний вісник університету/ Збірник наукових праць. Спец. Вип., том 2.- Переяслав-Хмельницький: П-Х ДПУ імені Г.Сковороди, 2010. - с.74-79.