20 години катедра "Търговски бизнес"

Стопанска академия „Д. А. Ценов" - Свищов

Факултет „Производствен и търговски бизнес"
Катедра „Търговски бизнес"

Юбилейна научнопрактическа конференция
с международно участие

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ТЪРГОВСКИЯ БИЗНЕС – КОМУНИКАЦИЯ МЕЖДУ НАУКА И ПРАКТИКА

Том II

12-13 май 2011 г.

Свищов, 2011 г.

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ" СВИЩОВ
ФАКУЛТЕТ „ПРОИЗВОДСТВЕН И ТЪРГОВСКИ БИЗНЕС"
КАТЕДРА „ТЪРГОВСКИ БИЗНЕС"

ЮБИЛЕЙНА НАУЧНОПРАКТИЧЕСКА КОНФЕРЕНЦИЯ
С МЕЖДУНАРОДНО УЧАСТИЕ

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ТЪРГОВСКИЯ БИЗНЕС КОМУНИКАЦИЯ МЕЖДУ НАУКА И ПРАКТИКА

12-13 май 2011 г.

Том II

20 ГОДИНИ
КАТЕДРА „ТЪРГОВСКИ БИЗНЕС"

Академично издателство „Ценов" Свищов
2011 г.

ОРГАНИЗАЦИОНЕН КОМИТЕТ

Председател: Доц. д-р Марияна Божинова

Членове: Доц. д-р Петранка Мидова
Доц. д-р Светослав Илийчовски
Доц. д-р Симеонка Петрова
Доц. д-р Теодора Филипова
Доц. д-р Петя Иванова

Конференцията се посвещава
на 20-годишния юбилей
на катедра „Търговски бизнес"
и на 75-годишнината от създаването
на Стопанска академия „Д. А. Ценов"
Свищов.

Публикуваните доклади не са редактирани и коригирани. Авторите носят пълна отговорност за съдържанието, оригиналността им и за грешки, допуснати по тяхна вина.

ISBN 978-954-23-0593-4

ЭКОСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проф. д. э. н. Сергей А. Охрименко
Лаборатория информационной безопасности
Молдавская Экономическая Академия – Кишинев, Молдова

Доц. д-р инж. Агоп С. Саркисян
Хозяйственная Академия имени Д. А. Ценова – Свиштов, Болгария

Введение

Проблема безопасности информационных и коммуникационных технологий, используемых в управлении, ставит все новые задачи по сохранению конфиденциальности, доступности и целостности информации и информационных ресурсов. Экономика развитых стран тесным образом связана с использованиебм информационных технологий. Производители вычислительной техники, программного обеспечения и, соответственно, предпринимательские структуры прилагают огромные усилия по созданию систем информационной безопасности, направленных на снижение рисков потерь информации, сбоев в работе вычислительных систем и сетей и т.д.

В настоящее время получили дальнейшее развитие технологии хранения и обработки информации. К их числу, в первую очередь, можно отнести виртуализацию, терминальный доступ, облачные вычисления, Web 2.0 и другие. Все новые технологии и средства требуют гарантий безопасности.

Одним из новых направлений совершенствования системы информационной безопасности является разработка основ экосистемы безопасности, которая представляет собой комплекс действий по предотвращению отрицательных последствий при использовании информационных технологий.

Безопасность „облачных вычислений”

Для обеспечения высокоэффективной защиты информационных ресурсов необходима реализация контроля на трех уровнях:

- контроль доступа к информации со стороны индивидуальных и коллективных пользователей информационной системы (обеспечение

доступа к информации авторизованным пользователям в нужный момент времени);

- контроль целостности и сохранности баз данных (обеспечение точности и полноты информации, а также методов ее обработки);

- контроль конфиденциальности передаваемых по сетям данных и подтверждения работоспособности сетевой инфраструктуры (обеспечение доступности информации только для тех, кто имеет соответствующие полномочия).

Данный подход сохраняется также и при использовании концепции „cloud computing”(облачные вычисления), которая представляет собой программно-аппаратное обеспечение, доступное пользователю через Интернет или локальную сеть в виде сервиса, позволяющего использовать удобный веб-интерфейс для удаленного пользователя к выделенным ресурсам. При этом компьютер пользователя выступает в качестве терминала для доступа к вычислительным ресурсам, программам и данным. Одновременно с этим, облачные вычисления являются методом расширения вычислительных мощностей без дополнительных инвестиций в новую инфраструктуру, обучение нового персонала и лицензирование нового программного обеспечения.

Новые реалии являются благоприятными для популяризации „облачных вычислений” и предусматривают:

- более массовое предложение;
- более понятный сервис для пользователей;
- более привлекательную функциональность;
- более доступную цену.

Рассмотрим кратко содержание данной концепции. Она объединяет несколько основных моделей, таких как, программное обеспечение как услуга, виртуализированные дата центры, интегрированная платформа для создания, тестирования и разработки собственных приложений, бизнес-аналитика как сервис, безопасность как сервис и др.

Основными преимуществами „Облачных вычислений” являются такие, как уменьшенная стоимость, увеличенный объем хранения данных, гибкость, высокая мобильность и т.д. В свою очередь, недостатками существующих подходов являются следующие: зависимость сохранности пользовательских данных от компании, предоставляющей данную услугу; появление монополистов в данной области; отсутствие единых стандартов; относительная нестабильная инфраструктура и т.д. Все основные недостатки, приведенные выше, характеризуются основным обстоятельством – относительно ранняя стадия развития кон-

цепции „облачных вычислений” и первоначальное накопление опыта эксплуатации.

В тоже время необходимо иметь в виду дополнительные преимущества: централизованное хранение данных; значительное сокращение времени при реагировании и расследовании инцидентов; сокращение времени тестирования безопасности; улучшение производительности приложений безопасности и др.

Концепция привносит и дополнительные риски безопасности:

- при централизованном хранении данных достаточно трудно организовать физический и логический контроль пользовательского доступа к данным, обрабатываемым за пределами компании;

- отсутствие общепринятых стандартов и процессов сертификации и аудита приводит к тому, что ответственность за безопасность и целостность данных лежит на владельце (клиенте), а не поставщике услуг;

- клиент может не владеть информацией относительно физического местоположения дата центра и юрисдикции страны размещения этого центра;

- данные клиента хранятся совместно в общей инфраструктуре с данными других клиентов, поэтому необходимо подтверждение, что выбранный и сконфигурированный алгоритм шифрования является эффективным;

- процессы восстановления данных в случае бедствия требуют разработки специальных решений по копированию данных и инфраструктуры для исключения полного отказа;

- необходимы дополнительные усилия по поддержке процессов логирования для безопасности приложений и данных;

- необходима поддержка различных форматов данных и приложений.

Специалисты в области информационной безопасности выделяют также ряд специфических проблем, требующих решения:

- все клиентские данные хранятся централизовано, что требует дополнительных гарантий в их сохранности;

- значительно повышается вероятность неавторизованных атак, как на данные, так и на приложения;

- отсутствует единый подход к построению платформы (использование поставщиками услуг, как открытого, так и закрытого формата;

- отдельной, практически неисследованной проблемой является построение бот-сетей на базе „облачных вычислений”.

Пользователи ожидают получить от использования данной технологии сокращение совокупной стоимости владения, повышение

эффективности и управляемости инфраструктурой, повышение устойчивости и надежности, сокращение парка серверов. Последнее обстоятельство является решающим в условиях возрастающей конкуренции. Но следует иметь в виду, что использование традиционных аппаратных и программных средств информационной безопасности не всегда приемлемо. Традиционные средства не гарантируют 100% безопасности.

На наш взгляд, возможны два пути в использовании средств защиты:

- во-первых, использовать только специализированные средства защиты, нечувствительные к угрозам виртуализации;
- во-вторых, использовать традиционные средства (например, управление доступом, криптография, антивирусы и др.) совместно с специализированным решением, предотвращающим угрозы виртуализации.

Экосистема информационной безопасности

В основу экосистемы положены этапы жизненного цикла уязвимости. Уязвимость – ошибка в программном обеспечении, которая может быть использована атакующим для доступа к системе и информационным ресурсам.

Модель жизненного цикла уязвимости включает следующие этапы:

- время создания;
- время открытия;
- время доступности;
- время общедоступного раскрытия;
- время доступности исправления;
- время инсталляции исправления.

В период между открытием уязвимости и ее устранением информационная система и ее ресурсы находятся в опасности. Данный период незащищенности может быть разбит на три дополнительные фазы:

- фаза предварительного раскрытия;
- фаза постраскрытия;
- фаза постисправления.

Модель экосистемы безопасности учитывает также наличие следующих игроков и стимулов: первооткрыватель уязвимости (физическое лицо, либо организация); рынок уязвимостей (открытый и „черный”); киберпреступники, использующие уязвимости; продавцы программного обеспечения; провайдеры и др.

Жизненный цикл уязвимости моделируется в зависимости от этапа „время доступности”, поскольку информация об уязвимости может стать недоступной для производителей и владельцев программного обеспечения и будет использоваться на „черном” рынке для извлечения прибыли, либо стать общедоступной, после чего последует комплекс действий по исправлению уязвимости. Приведенное выше описание является основой для формирования экосистемы безопасности, поскольку информация об уязвимости является ценным активом, как для владельца информационных ресурсов, так и для киберпреступника, который в состоянии использовать данную информацию как средство вымогательства и шантажа. Нельзя исключать возможности, что киберпреступники будут инвестировать значительные средства в процессы поиска неизвестных уязвимостей.

По нашему мнению, следует обратить пристальное внимание на складывающееся несоответствие между стандартом ISO/IEC 27001:2005, концепцией „облачных вычислений” и экосистемы информационной безопасности. В первую очередь, это относится к требованиям к системе менеджмента информационной безопасности.

Во-первых, организация должна управлять своими активами, что предусматривает инвентаризацию активов, определение ответственных лиц за активы, классифицировать активы по их значимости, правовым требованиям, важности и критичности, идентифицировать активы в соответствии с принципами классификации.

Во-вторых, находить и исправлять слабые места в системе информационной безопасности (устанавливать цели и планы, распределять ответственность в области информационной безопасности, обеспечивать ресурсами, принимать решения о приемлемых уровнях рисков и т.д.). В-третьих, регулярно проводить работы по выявлению угроз и уязвимостей в целях идентификации рисков (идентификация активов и соответствующих угроз и уязвимостей, определение возможных воздействий, реализация которых может привести к потере конфиденциальности, целостности и доступности ресурсов). В-четвертых, обеспечить эффективное управление в критических ситуациях, что предусматривает внедрение процессов непрерывности бизнеса, определение событий, влияющих на нарушение бизнес-процессов, разработку планов восстановления, тестирование и обновление планов.

Другими словами, отмеченные противоречия приводят к исключению риск-менеджмента, который по определению включает в себя анализ и оценку сильных и слабых сторон организации с точки зрения взаимодействия с различными контагентами.

Заключение

Представленный материал не исчерпывает всего многообразия проблем, связанных с реализацией новых технологий обработки и хранения информации и, соответственно, информационной безопасностью. Потребность в научных исследованиях и практической апробации отдельных разработок многократно возрастает.

Литература

1. R. Anderson and T. Moore, “The Economics of Information Security,”Science, vol. 314, no. 5799, pp. 610–613, 2006.
2. Sklavos N., Souras P. Economic Models and Approaches in Information Security for Computer Networks. International Journal of Network Security, Vol.2, No.1, PP.14–20, Jan. 2006.
3. Stefan Frei, Dominik Schatzmann, Bernhard Plattner, BrianTrammell. Modelling the Security Ecosystem – The Dynamics of (In) Security.
4. Охрименко С. А., Саркисян А. С. Подпольная информационная индустрия. Вісник економіки транспорту і промисловості № 29, 2010. Харьков, ХНЭУ, с. 19-22.
5. А. Саркисян, С. Охрименко Сенчестият пазар на информационни технологии. Приложна информатика и статистика – съвременни подходи и методи. Равда, 2009, с. 131-138.