СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ

Д.Г. Лобанова, Д.А. Диканева, Е.И.Качуров
Финансовый университет при Правительстве РФ, Москва, студенты
lobanova.dana@yandex.ru ,dasha.dikanyova@gmail.com

Аннотация. Специфические уязвимости облачных систем и методы их устранения. Факторы, затрудняющие защиту облачных сред. Факторы, которые необходимо учитывать при разработке адаптивных СПВ, необходимые функции. Возможные способы их модернизации.

Введение

Почему же именно облачные технологии так актуальны на сегодняшний день? Можно ожидать, что в скором времени IT трансформируется в сервис на подобии электричества, дав при этом мощнейший потенциал для инновационного развития. Поэтому ведущие компании-разработчики программного обеспечения направили свои усилия на создание средств защиты сред облачных вычислений. И одним из решений этой задачи могут стать адаптивные системы предотвращения вторжений в облачных системах.

Основные проблемы безопасности облачных вычислений

Ниже приведена классификация и описание основных проблем безопасности, которые возникают в облачной инфраструктуре. Мы определили следующие виды угроз для облака:

1. Неправомерное и нечестное использование облачных технологий
2. Небезопасные программные интерфейсы (API)
3. Внутренние нарушители
4. Уязвимости в облачных технологиях
5. Потеря или утечка данных
6. Кража персональных данных
7. Неправомерный доступ к сервису

Одним из факторов, затрудняющих защиту облачных сред, можно считать отсутствие:

- зрелых стандартов, классифицирующих облачные среды и регламентирующих их взаимодействие с другими системами;
- или недостаточный функционал защиты информации в интерфейсах прикладного программирования (API),
- устоявшейся практики реализации в облачных средах действующих ИБ-стандартов;
- организационной и технической возможности контроля состояния защищенности информации у клиентов.

Факторы, которые необходимо учитывать при разработке адаптивных систем

1. Ответственность.
2. Полнота контроля трафика.
3. Гибкость подхода: возможность модификации списка угроз.
4. Полнота видения/структура СПВ:
   a) уровень 1 – сеть
   b) уровень 2 – существующая инфраструктура.
   c) уровень 3 – развитие инфраструктуры.

Функции СПВ.

- Защита периметра облачной среды от сетевых атак.
- Поддержка согласованных функций обеспечения информационной безопасности в гибридных инфраструктурах: физической, виртуальной и облачной.
- Обеспечение эффективности эксплуатации благодаря поддержке согласованного адресного пространства между существующей физической и расширенной облачной инфраструктурой
- Сокращение общего времени развертывания полнофункциональной виртуальной машины за счет автоматического выделения IP-адресов быстро развертываемым виртуальным машинам.
- Унифицированные средства управления и мониторинга физических, виртуальных и облачных рабочих процессов.

Заключение

Переход на облачные вычисления обещает заманчивые возможности, как для компаний, предоставляющих интернет-услуги, так и для предприятий, активно использующих ИТ в своей работе. Сделав ставку на облачные вычисления, предприятия могут обеспечить себе экономию средств, гибкость и свободный выбор вычислительных мощностей. Возможности разрабатываемой интеллектуальной СПВ на облачные вычисления позволят повысить уровень информационной безопасности как имеющихся, так и перспективных корпоративных инфраструктур, интегрирующих облачные среды.

Список источников

1. http://blog.i-oblako.ru/
2. http://www.bureausolomatina.com/node/96
3. http://www.itland.com.ua/products/sect.php?SECTION_ID=291
4. http://www.pcweek.ru/security/article/detail.php?ID=139185