АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В «ОБЛАЧНЫХ» ВЫЧИСЛЕНИЯХ

Наумов А.Н.
Научный руководитель – доцент кафедры БИТ, к.т.н. Петренко О.Е.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр.Науки 14, каф.Безопасности информационных технологий, тел. (096)-220-54-86)
e-mail: num4ik@yandex.ru,

Cloud computing is one of the main focuses of development in infocommunications sphere of recent years. This is a technology of distributed data processing, in which computer resources and facilities are provided to the user as an Internet-service. However, due to the fact that the user does not own the infrastructure, a number of problems arise because the safety of user data depends on the provider. Cloud computing based on virtualization technology but this is the main cause of vulnerabilities.

Одним из основных направлений развития последних лет в мире инфокоммуникаций являются облачные вычисления. Это технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис. Однако, в связи с тем, что пользователь не является владельцем инфраструктуры, возникает ряд проблем, т.к. сохранность пользовательских данных напрямую зависит от провайдера.

Контроль и управление облаками является проблемой безопасности облачных вычислений. Гарантий, что все ресурсы облака посчитаны и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака нет. Это высокоуровневый тип угроз, т.к. он связан с управляемостью облаком, как единой информационной системой и для него общую защиту нужно строить индивидуально. В облачных вычислениях важнейшую роль платформы выполняет технология виртуализации.

Целью данной работы является анализ существующих способов обеспечения целостности и конфиденциальности данных в облачных вычислениях.

Для сохранения целостности данных и обеспечения защиты рассмотрим основные известные угрозы для облачных вычислений:

1. Трудности при перемещении обычных серверов в вычислительное облако.
2. Динамичность виртуальных машин.
3. Уязвимости внутри виртуальной среды.
4. Защита бездействующих виртуальных машин.
5. Защита периметра и разграничение сети.

Наиболее эффективные способы защиты в области безопасности облаков опубликовала организация Cloud Security Alliance (CSA). Проанализировав опубликованную компанией информацию, предложены следующие решения:

1. Шифрование – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным, должен шифровать информацию клиента, хранящуюся в центре обработки данных, а также в случае отсутствия необходимости, безвозвратно удалять.

2. Защита данных при передаче. Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения, даже в случаи доступа через ненадежные узлы. Такие технологии достаточно известны, среди них оптимальными для решения поставленных задач безопасности являются алгоритмы и надежные протоколы AES, TLS, IPsec.

3. Аутентификации — защита паролем. Для обеспечения более высокой надежности, лучшим вариантом является использования токенов и сертификатов. Для прозрачного взаимодействия провайдера с системой индетификациии при авторизации, также рекомендуется использовать LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language).

4. Изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальную сеть. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service). Часто провайдеры изолируют данные пользователей друг от друга за счет изменения данных кода в единой программной среде. Данный подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющему получить доступ к данным. В случае возможной ошибки в коде пользователь может получить данные другого.

Итак, описанные решения по защите от угроз безопасности облачных вычислений позволяют значительно снизить количество случающихся инцидентов. Но многие проблемы, связанные с защитой виртуализации до сих требуют тщательного анализа и проработанного решения.

Список источников:

1. Peter Mell, Timothy Gance. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, 2010.

2. Крупинин А. Cloud Computing: высокая облачность. Компьютерра, 2009.