МЕТОДЫ И МОДЕЛИ СИСТЕМНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНЫХ СЕРВИСАХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пруза́н А.Н.

Таболич Т.Г. – канд. техн. наук, доцент

Рассматривается информационная безопасность облачных вычислений

Облачные вычисления – это модель предоставления удобного сетевого доступа в режиме «по требованию» к коллективно используемому набору настраиваемых вычислительных ресурсов, которые пользователь может оперативно задействовать под свои задачи и высвобождать при сведении к минимуму числа взаимодействий с поставщиком услуги или собственных управленческих усилий [1]. Основным звеном для создания облачных платформ служит гипервизор. Гипервизор – это программа или аппаратная схема, обеспечивающая одновременный запуск сразу нескольких операционных систем на одном сервере виртуализации. В облачных вычислениях важнейшую роль платформы выполняет технология виртуализации. Для сохранения целостности данных и обеспечения защиты рассмотрим основные известные угрозы для облачных вычислений:

1. Трудности при перемещении обычных серверов в вычислительное облако. Требования к безопасности облачных вычислений не отличаются от требований безопасности к центрам обработки данных.
2. Динамичность виртуальных машин. Виртуальные машины динамичны.
3. Уязвимости внутри виртуальной среды. Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения [2].
4. Защита бездействующих виртуальных машин.
5. Защита периметра и разграничение сети [3].

Атаки на облачные сервисы и решения по их устранению:

1. Традиционные атаки на ПО. Уязвимости операционных систем, модульных компонентов, сетевых протоколов и др. — традиционные угрозы, для защиты от которых достаточно установить межсетевой экран, firewall, антивирус, IPS.
2. Функциональные атаки на элементы облака. Этот тип атак связан с многослойностью облака общим принципом безопасности.
3. Атаки на клиента. Большинство пользователей подключаются к облаку, используя браузер. Единственная защита от данного вида атак является правильная аутентификация и использование шифрованного соединения (SSL) с взаимной аутентификацией.
4. Атаки на гипервизор. Гипервизор является одним из ключевых элементов виртуальной системы. В качестве стандартных методов защиты рекомендуется применять специализированные продукты для виртуальных сред, интеграцию хост-серверов со службой каталога Active Directory, использование политик сложности и устаревания паролей, а также стандартизацию процедур доступа к управляющим средствам хост-сервера, применять встроенный брандмауэр хоста виртуализации [3];
5. Атаки на системы управления. Вмешательство в систему управления может привести к появлению виртуальных машин — невидимок, способных блокировать одни виртуальные машины и подставлять другие.

Наиболее эффективные способы защиты в области безопасности облаков:

1. Сохранность данных. Шифрование.Шифрование – один из самых эффективных способов защиты данных.
2. Защита данных при передаче. Зашифрованные данные при передаче должны быть доступны только после аутентификации.
3. Аутентификация. Аутентификации — защита паролем.
4. Изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальную сеть.

Список использованных источников:

1 Оттенхаймер, Дэви. Облачные вычисления: как соответствовать стандартам в облаке //Безопасность ИТ-структуры./ Дэви Оттенхаймер. – 2013. – № 1. –
2 Граннеман, Джозеф. Security as a Service: преимущества и риски безопасности на базе облака //Безопасность ИТ-структуры./ Джозеф Граннеман. – 2012. – № 11. – С. 9-14.
3 Шейклфорд, Дэйв. Защита информации в облаке: миссия выполнима //Безопасность ИТ-структуры./ Дэйв Шейклфорд. – 2012. – № 8. – С. 15-19.