УДК 004.021

М. В. Гладкий, магистрант; П. П. Урбанович, проф.
(БГТУ, г. Минск)

БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ НА ПЛАТФОРМАХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Одной из проблем в области практического использования облачных технологий является из безопасность. Следует постоянно модернизировать существующие и разрабатывать новые средства и механизмы защиты, способные обеспечить решение данной проблемы.

При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита более уязвимой части облака определяет общий уровень защищенности.

Можно провести следующую классификацию угроз в отношении облачных вычислений [1]:

- разграничение сети;
- динамичность виртуальных машин;
- уязвимости и атаки внутри виртуальной среды;
- защищенность данных и приложений;
- доступ системных администраторов к серверам и приложениям;
- защита бездействующих виртуальных машин;
- влияние традиционной безопасности на производительность;
- управление обновлениями.

Услуги по защите информации предлагают немало компаний. Но лишь некоторые из них этих предложений обеспечивают достаточно эффективную защиту, позволяющую в полном объеме обезопасить приложения от всех возможных видов атак. Данные атаки в зависимости от типа угроз и уровня воздействия можно разделить на следующие классы [2]:

- традиционные атаки на ПО;
- функциональные атаки на элементы облака;
- атаки на клиента;
- атаки на гипервизор;
- атака на виртуальные машины при их переносе с одного узла на другой;
- атаки на системы управления.

В свою очередь средства защиты в виртуальных средах можно условно подразделить на две группы.

К первой относятся средства защиты, которые поставляются в виде готовых аппаратных решений или в виде виртуальных устройств. Преимущества таких решений – быстрая скорость развертывания и

ввода в эксплуатацию, использование существующих аппаратных мощностей заказчика, экономия ресурсов (место в стойках, электропитание, кондиционирование) [3].

Вторую группу образуют средства, предназначенные для защиты непосредственно виртуальных машин и контроля коммуникаций в виртуальной среде (на уровне гипервизора). К ним относятся:

- межсетевые экраны (брандмауэры);
- средства обнаружения и предотвращения вторжений;
- средства контроля целостности;
- средства защиты от вредоносных программ, учитывающие виртуализацию;
- средства защиты от несанкционированного доступа;
- средства контроля политик безопасности в виртуальных инфраструктурах.

Основным преимуществом этих средств является специализация на защите виртуальных сред и коммуникаций в них. Среди производителей средств защиты для виртуальных сред можно отметить следующие компании: Trend Micro, Symantec, CheckPoint, StoneSoft, «Код Безопасности», Reflex Systems [4].

Рассмотренные в докладе методы и средства защиты имеют свои достоинства и недостатки. Зашифровав только одну часть облака, не предоставляется возможность защитить конференциальную информацию. Соответственно, для защиты данных на платформах облачных вычислений нужен комплексный подход, совмещающий использование шифрования с другими средствами защиты, включающих в себя программную реализацию межсетевого экрана, обнаружения и предотвращения вторжений, контроля целостности, защиты от вредоносного кода и анализа журналов.

ЛИТЕРАТУРА

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. Москва: ДМК Пресс, 2012.

2. Степаненко, В. Облачная обработка данных – миф или реальность? Москва: Сети и бизнес, 2010.

3. Риз, Д. Облачные вычисления. Санкт-Петербург: БХВ-Петербург, 2011.

4. Александров, А. Как предотвратить вторжение: второй уровень защиты. Москва: BYTE, 2009.