БЕЗОПАСНОСТЬ ОБЛАЧНЫХ РЕШЕНИЙ: ТИПОВЫЕ ПОДХОДЫ КРУПНЫХ ВЕНДЕРОВ

В.А. Розина, Е.В. Бегляк

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Вопросы безопасности являются основными препятствиями для широкого принятия облачных технологий. В данном докладе будут рассмотрены типовые подходы к безопасности облачных решений, а также механизмы обеспечения безопасности облачных инфраструктур и сервисов.

Защита памяти. Аппаратными средствами защиты являются: секционированный кэш (PC) и кэш с блокировкой по частям (PLC). В первом случае кэш динамически разбивается на защищенные области, которые могут быть специально сконфигурированы для конкретного приложения. Второй вариант предлагает изолировать только те строки кэша, которые содержат критические данные. Еще одним подходом является криптография. Одной из наиболее распространенных является Intel Advanced Encryption Standard (AES-NI), принципом действия которого заключается в аппаратной реализации некоторых подэтапов алгоритма AES.

Защита гипервизора. Защиты гипервизора от внедрения вредоносного кода включает в себя создание нескольких виртуальных машин клиента и их хранение в центральном хранилище. Также вендоры предлагают и базовые способы защиты, такие как системы мониторинга подозрительной активности:

– AWS CloudTrail;
– Azure Security Center;
– IBM Cloud Security Advisor.

Аутентификация и идентификация личности пользователей. Одна из проблем при использовании традиционных методов идентификации в облачной среде возникает, когда предприятие использует нескольких поставщиков облачных услуг. Это приводит к тому, что синхронизация данных о личности становится негибкой. Одним из подходов для решения данной проблемы является использование единой системы управления идентификацией и доступом (IAM). Некоторые крупные вендоры предлагают собственные решения IAM:

– Identity and Access Management от Amazon Web Services (AWS);
– IBM Cloud Identity and Access Management от IBM Cloud;
– Google Cloud Identity and Access Management от Google Cloud Platform (GCP).

Изоляция памяти. Изоляция памяти включает в себя использование техник, таких как Address Space Layout Randomization (ASLR) и CPU NX/XD, для предотвращения атак, основанных на переполнении буфера.

Изоляция устройств, сети. Изоляция устройств заключается в использовании механизмов виртуализации, таких как DMA-Remapping, позволяющих предотвратить несанкционированный доступ к физической памяти хостовой системы со стороны периферийных устройств с поддержкой DMA. Изоляция сети заключается в использовании виртуализированных сетевых контроллеров (vNIC) и межсетевых экранов, обеспечивающих контроль доступа и фильтрацию трафика между виртуальными машинами и внешней сетью,