УПРАВЛЕНИЕ ДОСТУПОМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Царегородцев Анатолий Валерьевич
д.т.н., профессор,
Финансовый университет при Правительстве РФ

Коростелев Антон Андреевич
аспирант,
Московский государственный институт электроники и математики
Национальный исследовательский университет
«Высшая школа экономики»

Введение

Управление доступом – обширная функция, которая включает в себя доступ требований для пользователей или системных администраторов (привилегированных пользователей), которые работают с сетью, системой или приложениями. Управление доступом в организации следует рассматривать согласно ее политики доступа и стандартов, принятых фирмой.

В модели облачных вычислений, где пользователи имеют доступ к облачным услугам с любого конечного устройства, имеющего доступ в Internet, роль сетевого контроля доступа значительно уменьшается. Причина в том, что стандартный контроль доступа сети фокусируется на защите ресурсов от несанкционированного доступа, основанного на атрибутах конечных устройств, которые в большинстве случаев неполноценны, не уникальны для различных пользователей и могут привести к неточной оценке. В облачных вычислениях сетевой контроль доступа проявляется в виде политики облачных брандмауэров.

В отличие от сетевого управления доступом, пользовательскому контролю доступа должно уделяться большее внимание в облачных вычислениях, так как это связано с идентификацией пользователя для доступа к ресурсам в облаках. Пользовательское управление доступом включает в себя строгую авторизацию, технологию единого входа (SSO), управление привилегиями, запись и мониторинг ресурсов облачных вычислений, играющих значительную роль в защите конфиденциальности и целостности информации в облачных вычислениях.

1. Контроль доступа SaaS

В модели поставки SaaS, CSP (криптопровайдер) отвечает за управление всеми аспектами инфраструктуры сети, сервера и приложений. В такой модели, где приложение поставляется как услуга для конечных пользователей, обычно через web-браузер сетеориентированные системы контроля становятся менее уместны и заменяются контролем доступа пользователя, например, при авторизации используются одноразовые пароли. Таким образом, следует обратить внимание на контроль доступа пользователей (авторизация, объединение, управление привилегиями, деинициализация и т.д.) для защиты информации, хранящейся в SaaS. Например, управление доступом в Salesforce.com организовано с помощью набора фильтров, которые поначалу кажутся простыми, однако это впечатление обманчиво. Каждый из фильтров применим к группам или классам пользовательских учетных записей.

1. Права класса пользователей на просмотр таблицы, объекта или функциональной области определяются профилями.

2. Права класса пользователей на просмотр столбца таблицы (атрибута объекта) определяются профилями.

3. Права класса пользователей на просмотр записи (строки или экземпляра) определяются ролями.

4. Типы записей определяют, каким профилям разрешено просматривать отдельные ячейки внутри записи, и могут использоваться для ограничения доступа практически к любой функции или классу объекта.

Эти фильтры имеют модификаторы, позволяющие делегировать права и расширять зону доступа для привилегированных пользователей. Впрочем, для большинства пользователей возможностей, предоставляемых механизмами фильтрации, оказывается вполне достаточно. Иногда это даже вызывает у них недовольство. Блокировки и фильтрации можно осуществлять в контексте текущего состояния и в зависимости от конкретных потребностей бизнеса. Таким образом, система позволяет задавать исключения при определении схемы совместного использования данных как на индивидуальном, так и на групповом уровне.

2. Контроль доступа PaaS

В модели PaaS, CSP отвечает за управление контролем доступа к инфраструктуре сети, серверов и платформенных приложений. Однако, клиенты отвечает за контроль доступа приложений, развернутых на PaaS платформе. Контроль доступа приложений проявляется как управление доступом конечного пользователя, что включает резервирование и аутентификацию пользователя.

3. Контроль доступа IaaS

В модели поставки IsaS, клиенты полностью несут ответственность в области управления всеми аспектами контроля доступа к их ресурсам на облаке. Доступ к виртуальным серверам, виртуальной сети, виртуальному хранилищу и приложениям, размещенным на IsaS платформе, должен быть разработан и организован клиентами.

В поставочной модели IsaS управление контролем доступа подразделяется на 2 вида:

- Контроль доступа на уровне инфраструктуры CSP (Управление контролем доступа к сети, размещению и управление приложениями, которые принадлежат и контролируются CSP);
- Контроль доступа на уровне виртуального клиента (Управление контролем доступа к вашему виртуальному серверу (виртуальной машине или VM), виртуальному хранилищу, виртуальным сетям и приложениям, размещенным на виртуальных серверах).

Принимая во внимание следующие аспекты в управлении контролем доступа инфраструктуры в облаке, как правило, рассматривается: сетевой контроль доступа, виртуальный контроль доступа к серверу, станцию управления облаком, web-консоль.

Заключение

Контроль доступа это важнейшая функция управления безопасностью в облачных моделях SPI (SaaS, PaaS, IaaS) и стандартной модели развертывания облака (публичная, частная и гибридная). Управление доступом является важным аспектом для защиты информации в информационных системах, построенных на основе облачных вычислений и может выступать основным средс-

твом управления безопасностью при отсутствии шифрования и других средств управления данными.

На данный момент возможности управления доступом, предлагаемые CPS, не являются достаточными для корпоративных клиентов по ряду причин:

- механизмы контроля доступа, нормы и процессы не стандартизированы посредством CSP. Для эффективного управления доступом к виртуальной облачной инфраструктуре клиентам необходимо предпринимать дополнительные усилия для понимания CSP параметров контроля доступа и их настройки;
- отсутствие единой стандартизации делает очень сложным управление доступом для нескольких облаков. Например, поддержка SAML не осуществляется с любого из главных CSP;
- контроль за доступом пользователя к ресурсам облака осуществляется на низком уровне. Контроль доступа с CSP обычно поддерживает управление на сетевом уровне, кроме управления доступом пользователей. Доступ пользователей относится к вопросам аутентификации. На мой взгляд, следует предложить гибкий контроль доступа, основанный на принципах наименьших привилегий и разделения обязанностей (например, консоль-менеджер, менеджер сетевого доступа, хост-менеджер).

С точки зрения корпоративных клиентов управление доступом это основной процесс обеспечения безопасности для защиты конфиденциальности, целостности и доступности информации, расположенной в облаке. Надежная программа управления доступом должна включать в себя резервное копирование, время деинициализации, гибкую аутентификацию, управление привилегиями, учет использования ресурсов, аудит и поддержка соответствующего управления. Клиенты облака должны понимать CSP-специфичные особенности контроля доступа для сетей, систем и приложений.

Список источников

1. Tim Mather, Subra Kumaraswamy, Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance // O'Reilly Media, Incorporated, 2009.