СРЕДСТВА ЗАЩИТЫ ДАННЫХ ПРИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Стиняева В.М.

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

Ганжа В.А. – к.т.н.,доцент

Управление, а также контроль над облаками — является проблемой безопасности и сохранности данных. Гарантий, что все ресурсы облака используются по назначению и в нем нет неуправляемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака нет. Поэтому рассмотрим основные и актуальные способы защиты данных при облачных вычислениях.

Для контроля безопасности в облаках необходим комплексный подход в обеспечении как физической, так и сетевой безопасности. В основе обеспечения физической безопасности лежит строгий контроль физического доступа к серверам и сетевой инфраструктуре. А сетевая безопасность представляет собой построение надежной модели угроз, включающей в себя защиту от вторжений и межсетевой экран. Использование межсетевого экрана подразумевает работу фильтра, с целью разграничить внутренние сети центра обработки данных (далее – ЦОД) на подсети с разным уровнем доверия.

Наиболее эффективными способами обеспечения безопасности при облачных вычислениях являются:

1) шифрование – один из эффективнейших способов защиты данных. Провайдер, предоставляющий доступ к данным, шифрует данные клиента, хранящиеся в ЦОД, а также в случае отсутствия необходимости, безвозвратно удаляет их. Таким образом, облако всегда имеет дело только с зашифрованными данными.

Выделим плюсы шифрования данных:

- провайдер не сможет получить доступ к данным клиента;
- никакой элемент на пути следования трафика не получит доступ к данным клиента (например владелец wi-fi точки какого-либо заведения).

Главным условием с целью предоставления защищенности подобного решения считается отдельное использование облачного сервера и сервера управления ключами (рисунок 1);

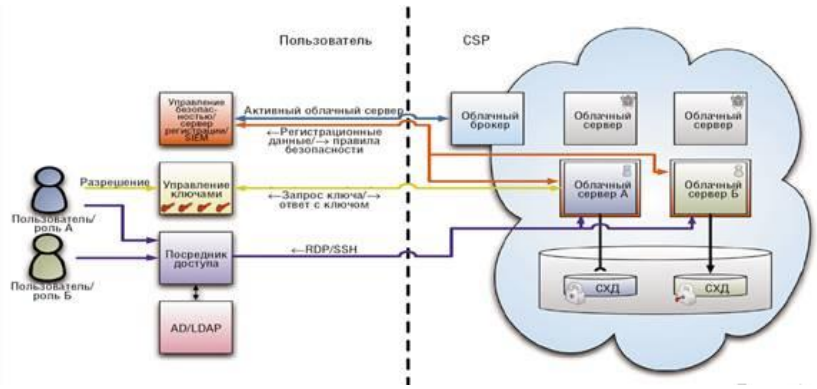

Рисунок 1 - Схема взаимодействия пользователя, сервера управления ключами и облачного сервера

2) защита данных при передаче. Зашифрованные данные при передаче в облако и при хранении в нем должны быть доступны только после аутентификации. Это позволят обеспечивать конфиденциальность данных даже если кто-то получит к ним доступ посредством ненадежных узлов в сети. Применяются такие алгоритмы и протоколы как AES, TLS, IPsec. Также для публичных облаков используется VPN-туннель, основанный на двухфакторной аутентификации;
3) аутентификация — процесс подтверждения подлинности субъекта. Для более высокой надежности прибегают к использованию сертификатов, токенов и двухфакторной аутентификации. Для прозрачного взаимодействия провайдера с системой индетификациии при авторизации, также рекомендуется использовать стандарты LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language);
4) изоляция пользователей. Самым актуальным и надежным способом изоляции пользователей является 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);

Таким образом можно подытожить, что обеспечение информационной безопасности при использовании облачных вычислениях зависит и от клиента, и от провайдера. Следует подойти серьезно к составлению договора с поставщиком облачных услуг и учесть все факторы, которые могут повлиять на обеспечение конфиденцианости данных. Со стороны клиента - это использование современных программных и аппаратных средств, работа профессионально подготовленного персонала, обеспечение безопасности сетевого оборудования, хранилища данных, сервера и гипервизора. Дополнительно возможно размещать в выделенном ядре антивирус для предотвращения заражения гипервизора через виртуальную машину, систему шифрования данных для хранения пользовательской информации в зашифрованном виде и средства для реализации зашифрованного тунелирования между виртуальным сервером и клиентской машиной. Также проводить своевременный аудита всех систем на выявление уязвимостей и контроль уровней доступа пользователей.

Список использованных источников:

1. Котяшичев И. А., Бырылова Е. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. — 2015. — №6.4. — С. 30-34. — URL https://moluch.ru/archive/86/16357/ (дата обращения: 24.03.2019).
2. Удо Шнайдер Использование облачных сервисов [Текст] / У. Шнайдер //
3. Информационная безопасность в облачных вычислениях: уязвимости, методы и средства защиты, инструменты для проведения аудита и расследования инцидентов URL: https://www.bibliofond.ru/view.aspx?id=783809 (дата обращения: 24.03.2019)
4. Арзамасов Е.В., Чурикова А.А. Угрозы облачных вычислений и методы их защиты // Технические и математические науки. Студенческий научный форум: электр. сб. ст. по мат. V междунар. студ. науч.-практ. конф. № 5(5). URL: https://nauchforum.ru/archive/SNF_tech/5(5).pdf

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ МЕТОДОМ АНАЛИЗА ДИНАМИКИ ВВОДА ТЕКСТА

Супринович И.Ю.

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

Искра Н.А. – старший преподаватель

В данной работе рассматриваются алгоритмы идентификации пользователя методом анализа динамики ввода текста. Помимо этого рассматривается возможность и сценарии применения этого метода идентификации, а также изучаются способы классификации, которые позволят сделать идентификацию пользователя более точной.

Потребность в распознавании людей по каким-либо уникальным, присущим только им признакам, возникла достаточно давно. Эту проблему призвана решить аутентификация — процесс идентификации и подтверждения личности пользователя. Обычно он сопровождается авторизацией, которая является механизмом определения того, какими правами наделяется пользователь после идентификации.

Аутентификация классифицируется следующим образом:

1) аутентификация на основе уникальной информации — для успешной идентификации пользователю необходимо ввести пароль;

2) аутентификация на основе уникального предмета — для успешной идентификации пользователю необходимо предъявить уникальный предмет, например пластиковую карту;

3) аутентификация на основе какой-либо уникальной характеристики пользователя, физиологической или поведенческой (биометрия).

Одним из представителей поведенческой биометрии является аутентификация методом анализа динамики ввода текста (АМАДВТ) — распознавание пользователя с помощью анализа динамики ввода текстовых последовательностей. Данный метод считается достаточно надёжным, так как очень сложно изучить темп и стиль ввода другого человека. Также он не требует какого-либо специального оборудования в отличие от методов физиологической биометрии.

В основе АМАДВТ лежат алгоритмы выявления аномалий — алгоритмы, позволяющие выделить необычные значения в выборке данных. От выбора алгоритма зависит точность распознавания пользователя. Наиболее часто используемыми метриками для выявления аномалий являются стандартное расстояние Махалонобиса, а также его разновидности — фильтрованное и масштабированное.