III. Проблемы обеспечения информационной безопасности

Курако Е.А., Орлов В.Л.

Организация защиты в информационных системах, ориентированных на облачную технологию

Аннотация: Рассматривается использование средств защиты информации в системах, строящихся с использованием облачных технологий. Определяются основные угрозы и анализируются методы обеспечения безопасности.

Ключевые слова: информационные системы, сеть, облако, защита информации, удаленный доступ

В настоящее время использование облачных технологий непрерывно расширяется. Напомним, что «облака» вначале получили массовое распространение как внешние хранилища информации, которую пользователь не может разместить у себя на компьютере, например, ввиду большого объема. Поэтому он получал возможность доступа к внешнему хранилищу, в которое можно перемещать свои данные, в основном, для временного хранения. Уже на начальных стадиях стала использоваться парольная защита доступа к облачному хранилищу и затем – шифрование информации. Причем услугу шифрования начали предлагать организаторы «облаков».

На следующей стадии развития – облачные структуры стали предоставлять функцию обмена информацией между различными пользователями. Это являлось естественным продолжением идеи облачных хранилищ. Действительно, если присутствуют в Интернет-пространстве области для размещения информации, то возможно организовать доступ к этим областям или, точнее к их фрагментам для нескольких пользователей. При этом владелец хранилища может дать право для работы с тем или иным файлом (или группой файлов) другим пользователям, выделяя подмножество привилегированных пользователей или разрешая

открытый доступ к файлу неограниченному числу пользователей, то есть по существу – проводя открытую публикацию.

В последнем случае ни шифрование, ни пароль не требуются, и осуществляется защита только от модернизации опубликованного файла. То есть, разрешается доступ по чтению, копированию, но запрещается доступ по изменению.

Следующим шагом должен был являться переход к санкционированному изменению данных, размещенных в облаке. И такой шаг был сделан. Появились системы, определяемые аббревиатурой SaaS (software as a service – программное обеспечение как услуга). Взаимодействие между компонентами такой системы представлено на рис.1 в виде упрощенной модели.

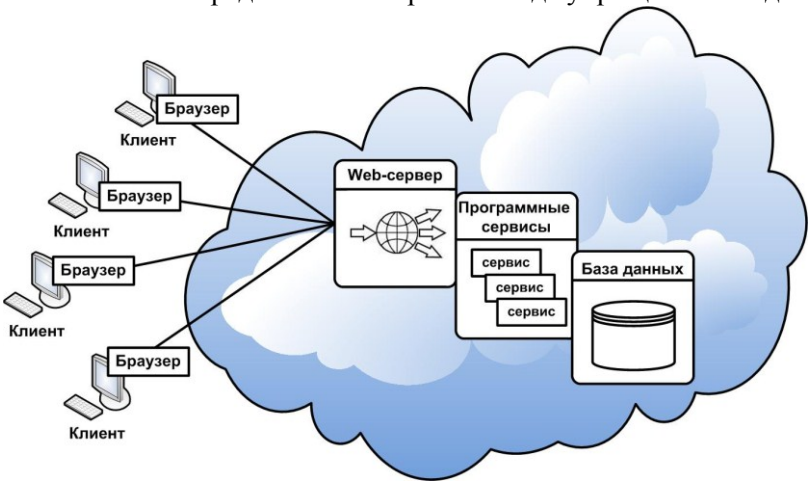

Рис. 1 – Взаимодействие в SaaS-модели

SaaS-системы не только обеспечивают хранение информации в облаке, но и позволяют изменять их [1]. В таких системах обрабатываются внешние запросы разного назначения, в результате выполнения которых данные не только копируются в хранилище и выбираются из него, но и создаются новые данные, а в результате системной обработки, организуется просмотр и извлечение информации.

В SaaS-модели обращение от клиентской программы (в качестве которой обычно выступает браузер) идет, как правило,

через web-сервер к программным сервисам, которые обращаются к хранилищу информации. Разумеется, реальные SaaS-системы могут быть устроены по-разному. Например, в качестве программных сервисов могут выступать SOAP-сервисы, REST-сервисы и другие программные средства. Хранилище может быть представлено просто файлами. Но в крупных системах используется хранилища информации, управляемые СУБД, например, PostgreSQL.

Рассмотрим возможные угрозы безопасности, которые характерны для таких систем. Предполагаемых нарушителей здесь можно разделить на три категории: внешний, внутренний и поставщик. Если с первыми двумя категориями все понятно, это люди, не имеющего прямого доступа к системе или имеющие доступ частичный/полный к функциям системы. Поставщик - это нарушитель из персонала организации, предоставляющей в аренду облачные ресурсы. То есть он не имеет доступа к функциям системы, но имеет доступ к операционным системам, системам управления базами данных и к другим серверным компонентам.

На основе анализа проблем безопасности в облаке [2, 3] представим перечень основных угроз со стороны этих нарушителей для систем типа SaaS в виде таблицы 1.

Из таблицы 1 следует, что одной из основных угроз является кража данных. Для уменьшения вероятности этого события относительно внешнего нарушителя можно сделать следующее:

шифровать информацию, передаваемую по линиям связи с использованием технологии http;

при входе в серверную часть использовать Firewall для фильтрации информационного потока;

обеспечить разграничение доступа в информационной системе, с тем, чтобы даже при подключении к системе от имени того или иного пользователя обеспечивался доступ к ограниченной информационной области.

Таблица 1

Основные угрозы в облачной структуре

Основные угрозы	Нарушитель	Основные меры защиты
Кража данных	Внешний, Внутренний Поставщик	Https, Firewall, разграничение доступа

Основные угрозы	Нарушитель	Основные меры защиты
Потеря данных	Поставщик	Резервирование данных
Кража и раскрытие аккаунтов	Внешний, Внутренний	Надежная двухфакторная аутентификация
Незащищенные интерфейсы и API	Внешний	Https, разграничение доступа к ресурсам
DDoS-атаки	Внешний	Фильтрация атак
Злонамеренный инсайдер	Внутренний	Логирование, мониторинг, аудит событий
Уязвимость используемых систем	Внешний, Внутренний	Применение последних патчей, своевременное обновление

Как уже отмечалось, что здесь появляется еще один вид нарушителя – поставщик облачной инфраструктуры, на оборудовании которого и размещается база данных (БД). У клиентов именно эта угроза вызывает наибольшие опасения, так как их данные находятся у поставщика.

Чтобы ограничить сотрудникам поставщика доступ к БД предлагается блокировать им прямой доступ к паролю базы данных. То есть пароль не должен никто знать, кроме программ, которые работают с этой БД. Именно поэтому любая из доверенных программ при обращении каждый раз вычисляет значение пароля с использованием хеш-преобразования на основании идентификационных данных этой БД и последовательности символов, известных только программе, которая обычно называется «соль».

Такой подход ограждает также от атак к базе данных со стороны внутренних и внешних нарушителей, так как пароль БД нигде не хранится и неизвестен персоналу.

Также важно построение «двухслойных» облаков. При этом в компьютерах первого слоя расположены только программные средств, в то время как все данные размещены во втором слое, доступ к которому ограничен. Поэтому от внешнего мира все данные ограждены за счет наличия первого слоя, снабженного соответствующими средствами безопасности.

Возможная потеря данных также является существенной угрозой. Обычно за функции восстановления отвечает поставщик, который делает резервные копии и может обеспечить

восстановление БД в случае аварии. При этом наряду с копией БД могут использоваться также журналы.

Простой пароль пользователя может быть легко подобран. Поэтому он должен быть достаточно сложен. Рекомендуется использовать также двухфакторную аутентификацию [4], так как при повышении надежности представления здесь существенно труднее осуществить похищение идентификационных данных. Нужно украсть не только пароль, но и физической носитель информации (например, sim-карту телефона).

Построение надежных интерфейсов и API с ограниченной функциональностью зависит от разработчика. В частности, для обеспечения надежного интерфейса может быть рекомендован сервис-браузер [5, 6].

Ddos-атаки – это атаки типа «отказ в обслуживании», которые приводят к фактической невозможности использования системы. Большинство этих атак должны отражаться средствами поставщика.

Злонамеренный инсайдер может появиться среди уволенных сотрудников, доступ которого к системе своевременно не заблокирован. Также нарушителем такого рода может стать администратор системы, который имеет доступ к множеству ресурсов. Способ борьбы с этими атаками в основном состоит в журналировании всех ключевых событий, мониторинге и анализе ситуации в процессе аудита.

Атаки также могут появляться за счет использования уязвимостей операционных систем и прикладных программных комплексов. Основные средства борьбы с ними – это своевременное обновление программ.

Таким образом, современные средства безопасности позволяют использовать облачные технологии для построения информационных систем. Системы, построенные таким образом, имеют ряд особенностей, отмеченных выше, что требует их учета в процессе проектирования.

Литература:

1. *Денисов Д.В.* SaaS-решения лидеров IT-индустрии. // Прикладная информатика. – 2010. – №1(25). – С.35-43.

2. Угрозы безопасности в облаке [Электронный ресурс]. – Режим доступа:http://www.tadviser.ru/index.php/Статья:Главные_угрозы_без

опасности_в_облаке. – Заглавие с экрана. – (Дата обращения: 15.10.2019).
3. ТОП-12 угроз облачной безопасности по версии Cloud Security Alliance [Электронный ресурс]. – Режим доступа: https://iaas-blog.it-grad.ru/bezopasnost/top-12-ugroz-oblachnoj-bezopasnosti-po-versii-cloud-security-alliance/– Заглавие с экрана. – (Дата обращения: 16.10.2019).
4. *Козлов А.Д., Орлов В.Л.* Методы и средства обеспечения информационной безопасности распределенных корпоративных систем. – М. ИПУ РАН, 2017. – 156 с.
5. *Курако Е.А., Орлов В.Л.* Сервис-браузеры для информационных систем // Программная инженерия. – Москва, 2017. – Том 8, №9. – С. 413-421.
6. *Курако Е. А., Орлов В. Л.* Способ организации взаимодействия клиента с сервером приложений с использованием сервис-браузера: Патент на изобретение RU 2656735 C1; Зарегистрирован 06.06.2018. Заявлено 17.05.2017. Опубликовано: 06.06.2018 Бюллетень № 16.