П. В. Ивонин

БЕЗОПАСНОСТЬ ОБЛАКА В ДЕТАЛЯХ

Не секрет, что облачные технологии сейчас находятся на волне популярности: экономичность, легкость развертывания, многопользовательская архитектура — все это способствует быстрому распространению облаков и захвату ими большей части рынка ИТ. Экономичность облаков делает их особенно популярными для хранения информации. Компании также используют публичные облака для проектов, требующих временных или переменных вычислений, из-за подхода к оплате «плати лишь за использование». Они могут использовать публичные облака вместо того, чтобы настраивать собственную внутреннюю инфраструктуру только лишь для частичного или временного использования. Но облачная инфраструктура также представляет повышенные риски и более ограниченную возможность контроля. В этом и заключаются главные проблемы облачных вычислений — защита информации и доверие пользователей по отношению к облачным провайдерам.

Как же убедить клиента, что его данные будут в безопасности? Решением является соответствие облака требованиям нормативных документов и стандартов в области обеспечения информационной безопасности. Но в российском законодательстве пока нет стандартов, описывающих принцип построения защиты информации в облачных вычислениях. Вследствие этого поставщики облачных услуг вынуждены сами выбирать способы защиты информации из огромного количества готовых решений, представленных на рынке. Но все средства защиты должны учитывать особенности облачной технологии [1].

Ключевыми элементами облачной системы являются гипервизор, управляющий виртуальной средой облака, центр обработки данных, на котором содержится большая часть конфиденциальной информации, канал связи между потребителем облачного сервиса, а также ПО, установленное на компьютере потребителя (в частности, интернет-браузер).

Все перечисленные элементы могут быть подвержены атакам со стороны злоумышленника. При успешной атаке на любой из элементов облачной системы каждый аспект безопасности информации (конфиденциальность, целостность, доступность) может быть нарушен.

На подход к безопасности влияет также передача конфиденциальных данных незаинтересованной стороне, что обусловливает необходимость дополнительных протоколов взаимодействия между поставщиком облачных услуг и их потребителем.

Специфика облачных вычислений с точки зрения безопасности информации:

- хранение данных у незаинтересованной стороны;
- контроль и управление безопасностью по требованию;
- выявление нарушений в режиме реального времени;
- быстрое восстановление работоспособности сервисов;
- необходимость подготовки квалифицированных специалистов
- по безопасности облачных систем;
- значительные инвестиции в инфраструктуру безопасности.

Как и любая другая система, функционирующая посредством сети Интернет, публичное облако подвержено атакам. Основные виды атак, присущих облачным технологиям, приведены ниже:

- традиционные атаки на ПО;
- атаки на клиента;
- сетевые атаки;
- атаки на серверы облака;
- реализация комплексных угроз.

Для обеспечения информационной безопасности облаков система защиты информации должна включать в себя:

- подсистему обеспечения безопасности информации на стороне клиента;
- подсистему обеспечения сетевой безопасности;
- подсистему обеспечения безопасности виртуальных сред;
- подсистему обеспечения безопасности центров обработки данных.

Как и в любой другой системе защиты информации, безопасность системы в целом зависит от безопасности всех ее частей. Далее подробнее рассмотрим каждую подсистему в отдельности.

Подсистема обеспечения безопасности информации на стороне клиента

Пользователи работают с сервисом облачных вычислений с помощью интернет-браузера, поэтому подвержены таким атакам, как Cross-site-scripting (XSS), Phishing, а также вирусы и трояны.

Таким образом, подсистема обеспечения безопасности информации на стороне клиента состоит из следующих элементов:

a) антивирусные средства защиты информации;

b) средства шифрования данных на диске;

c) встроенный в ОС персональный брандмауэр;

d) безопасно настроенный интернет-браузер.

Подсистема обеспечения сетевой безопасности

В целях защиты данных в публичном облаке используется туннель виртуальной частной сети (VPN), связывающей клиента и сервер для получения публичных облачных услуг. VPN-туннель способствует безопасным соединениям и позволяет использовать единое имя и пароль для доступа к разным облачным ресурсам. В качестве средства передачи данных в публичных облаках VPN-соединение использует общедоступные ресурсы, такие как Интернет. Процесс основан на режимах доступа с шифрованием при помощи двух ключей на базе протокола Secure Sockets Layer.

Подсистема обеспечения безопасности виртуальных сред

Безопасность виртуальной среды зависит от безопасности механизмов виртуализации.

При успешной атаке на гипервизор нарушитель может незаметно для традиционных СЗИ, работающих в виртуальных машинах:

- копировать и блокировать весь поток данных, идущий на все устройства (HDD, принтер, USB);
- читать и изменять данные на дисках виртуальных машин, даже когда они выключены и не работают, без участия программного обеспечения этих виртуальных машин.

Для защиты гипервизора необходимы разграничение прав доступа к серверу виртуализации, своевременная установка обновлений ПО среды виртуализации, ограничение запуска программ.

Виртуальная машина исполняется на сервере виртуализации, а ее диск хранится на SAN/NAS. Следовательно, необходимо защитить данные виртуальных машин путем разграничения доступа к дискам виртуальных машин, реализуемого сертифицированными СЗИ от НСД и межсетевыми экранами, контролирующими протоколы и файловые форматы виртуальной инфраструктуры [2].

Получив доступ к средствам администрирования, нарушитель имеет возможность/может похитить, уничтожить или исказить любые данные во всей виртуальной инфраструктуре. Необходима защита периметра сети администрирования путем разграничения доступа к серверам виртуальных машин и средствам управления инфраструктурой.

Виртуальные машины одного физического сервера могут обмениваться трафиком напрямую, без участия физических сетевых коммутаторов. Таким образом, использование физических межсетевых экранов не будет эффективным. Нужна модернизация существующих сертифицирован-

ных межсетевых экранов, их перенос в виртуальную среду, а также создание специализированных СЗИ от НСД и межсетевых экранов, контролирующих трафик внутри сервера виртуализации.

По сети репликации виртуальных машин передаются сегменты их оперативной памяти. Возможность перехвата этих данных — прямая угроза безопасности. Сеть репликации должна быть изолирована от других сетей, а также необходимо использовать сертифицированные VPN для канала репликации.

Простота создания и ввода в эксплуатацию виртуальных машин может привести к проблемам для безопасности, если к ним не применяется политика безопасности.

Требуется организация централизованного процесса управления жизненным циклом виртуальных машин, согласующегося с политикой безопасности организации [3].

Подсистема обеспечения безопасности центров обработки данных

Центр обработки данных (ЦОД) обеспечивает гарантированную безотказную работу информационной системы с заданными уровнями безопасности, надежности и доступности. Использование такой технологии позволяет создавать резервные хранилища данных без потери функциональности информационной системы.

Традиционный ЦОД представляет собой кластер серверов, созданный с целью повышения эффективности и защищенности. Защита ЦОД подразумевает физическую и сетевую защиту.

Основными объектами защиты в ЦОД являются оборудование, конфиденциальная информация и ПО. Подсистема обеспечения безопасности центров обработки данных включает в себя следующие элементы:

- охранное видеонаблюдение;
- охранно-пожарная сигнализация;
- система контроля и управления доступом;
- система резервного копирования и восстановления данных;
- система защиты информации в ЦОД.

Системы охранного видеонаблюдения позволяют сотрудникам службы безопасности осуществлять визуальный контроль обстановки на объекте. Видеонаблюдение дает возможность не приставлять к каждому серверу своего охранника: контроль объекта ведется дистанционно, круглосуточно, без выходных и праздников. Кроме того, запись видео с камер позволяет в любое время организовать просмотр того или иного инцидента с целью выявления нарушения.

При обеспечении безопасности ЦОД должно уделяться внимание таким угрозам, как пожар, задымление и т. п., и необходимо оперативное оповещение о них сотрудников организации и службы безопасности. Следовательно, автоматическая система пожаротушения — один из самых эффективных методов экстренного пожаротушения. Данная система воздействует на очаг возгорания еще в процессе его зарождения, позволяет избежать распространения огня на большой площади и, соответственно, минимизирует ущерб.

Система контроля и управления доступом осуществляет автоматическое управление входами-выходами и призвана разграничивать доступ людей на определенные территории, вести подсчет посетителей, фиксировать их перемещения по территории и т. д. Система также способна распознавать лица, цвета, автомобильные номерные знаки и т. п. и на основе полученной информации принимать решение о доступе объекта или предмета, обладающего данными признаками, к определенной зоне [4].

ЦОД обеспечивает построение высоконадежных систем хранения данных. Реализуются технологии распределенной сети хранения данных. С целью защиты данных от физического или логического повреждения выполняются работы по созданию систем резервного копирования и репликации в них данных.

Системы резервного копирования и архивирования обеспечивают сохранность критической для бизнеса компании информации, оптимальное соотношение времени восстановления и момента восстановления данных, минимизируют влияние человеческого фактора на процедуры резервного копирования.

В качестве компонентов системы информационной безопасности ЦОД должны выступать следующие элементы:

1. система централизованного управления средствами защиты информации;
2. средства обнаружения и предотвращения вторжений;
3. средства антивирусной безопасности;
4. средства криптографической защиты информации (шифрование файлов и работа с ЭЦП, прозрачное шифрование жестких дисков, шифрование выбранных полей в БД);
5. средства межсетевого экранирования;
6. средства разграничения доступа;
7. средства мониторинга и управления событиями;
8. средства контроля целостности информации и приложений.

Облачные вычисления представляют собой значительный прогресс в сфере развития информационных технологий и сервисов. Обеспечивая по требованию пользователя доступ к общим источникам вычислительных ресурсов в автономном, динамично масштабируемом и выверенном режиме, облачные вычисления предлагают очевидные преимущества в скорости, оперативности и эффективности.

В данной технологии безопасность играет важнейшую роль, этой проблеме специалисты уделяют особое внимание. Но, несмотря на все сложности в области безопасности, преимущества предоставляемых через Интернет сервисов перевешивают возможные риски и облачные вычисления будут широко востребованы на рынке информационных технологий.

СПИСОК ЛИТЕРАТУРЫ:

1. *Peter Mell, Thimothy Grance*. «The NIST Definition of Cloud Computing (Draft)» // Recommendations of the National Institute of Standards and Technology, Special Publication 800 – 145 (Draft), сентябрь 2011 год.
2. *Ширманов А*. Безопасность виртуализации при обработке данных ограниченного доступа // Москва, ЭКСПОЦЕНТР, InfoSecurity Russia. 30 сентября 2009.
3. *Лаборатория Касперского*. «Что такое фишинг». URL: http://www.securelist.com/ru/threats/spam?chapter=164 (дата обращения: 12.04.2013).
4. *Флайлинк*. «Безопасность ЦОД». URL: http://www.flylink.ru/info/articles/553/1404 (дата обращения: 12.04.2013).