Периметр в облаке – он есть или его нет?

Владимир Воротников, *руководитель отдела перспективных исследований и проектов ЗАО "С-Терра СиЭсПи"*

К понятию облачных технологий сейчас относят зачастую избыточное количество технологий. Как следствие, количество новой терминологии зашкаливает, и к тому же она далеко не всегда согласована между различными вендорами. Это не способствует пониманию происходящего у рядовых администраторов и инженеров. Непонимание, как любая неопределенность, вызывает тревогу и страх.

За облаками всегда скрывается солнце

Одной из популярных тем, активно обсуждаемых в последнее время в IT-сообществе, является безопасность облачных сред. Некоторые предпосылки к таким активным обсуждениям очевидны. С одной стороны, в облачных технологиях возникает большое число новых угроз, с другой – сама суть облачных технологий подразумевает консолидацию большого количества информации и ресурсов в одном месте, что повышает ответственность за их безопасность. Есть и менее очевидные предпосылки. Например, к понятию облачных технологий сейчас относят огромное, зачастую избыточное количество технологий. Как следствие, количество новой терминологии зашкаливает, и к тому же она далеко не всегда согласована между различными вендорами. Это не способствует пониманию происходящего у рядовых администраторов и инженеров. Непонимание, как любая неопределенность, вызывает тревогу и страх. А дальше действует положительная обратная связь: множественные статьи и обсуждения безопасности облаков вызывают ощущение непреодолимости и чудовищного масштаба проблемы, что вызывает еще больший страх. Мне бы хотелось приободрить коллег и напомнить, что за облаками всегда скрывается солнце.

Классический защищенный сегмент сети похож на средневековую крепость: стены крепкие, все входы и выходы известны, внутри – все свои, проверенные люди. Сегмент сети в облаке, в таком случае, больше похож на хостел: в вашей комнате какие-то незнакомые соседи, которые меняются каждый день. Двери вроде как запираются, но ключи от всех дверей есть у администрации, да еще и эту самую администрацию вы в лицо не знаете. Тревожное место.

Многовековая защита

Многие тысячелетия природа учила человека строить укрытия. Огородил вход в пещеру – внутри безопасно. Обнес замок высокой стеной – и чувствуешь себя защищенным. Неудивительно, что по тому же принципу человек начал строить защиту своих данных. Серверная – закрытое помещение, которое запирается на ключ, следовательно, физически данные защищены, можно быть спокойным. Есть только один выход для данных наружу – через канал провайдера, и он закрывается межсетевым экраном. Тут становится немного тревожнее. Подсознание, конечно, больше доверяет дверям и ключам, чем странному металлическому аппарату с проводами. Но паники пока не возникает. Все-таки защитника своих данных видно (вон он в стойке мигает лампочками) и его даже можно потрогать рукой. А если что – всегда можно взять и отрезать канал провайдера ножницами по металлу. Во избежание, так сказать.

Таким образом, человек вообще и инженер в частности всю свою жизнь привык огораживать ценные для себя вещи и данные реально осязаемыми системами защиты, принадлежащими только ему. Это четкое понимание наличия границы, или периметра, все входы и выходы из которого понятны, дает ощущение если не безопасности, то, по крайней мере, контролируемости ситуации.

Хостел или банк?

Совсем по-другому дела обстоят в случае применения облачных технологий. Больше нельзя понять, где конкретно находятся твои данные. Некоторые авторы утверждают, что периметр пропадает, но я с этим не соглашусь. Периметр остается. Но он, во-первых, становится динамическим, постоянно меняющимся, как и само пространство вашего контроля, которое постоянно меняется. Во-вторых, в периметре появляется намного больше дверей, причем большинство из них человек не в силах увидеть глазами и пощупать руками, их можно только осознать мозгом.

Здесь, мне кажется, уместна следующая аналогия. Классический защищенный сегмент сети похож на средневековую крепость: стены крепкие, все входы и выходы известны, внутри – все свои, проверенные люди. Сегмент сети в облаке, в таком случае, больше похож на хостел: в вашей комнате какие-то незнакомые соседи, которые меняются каждый день. Двери вроде как запираются, но ключи от всех дверей есть у администрации, да еще и эту самую администрацию вы в лицо не знаете. Тревожное место. Студенту переночевать – пойдет. Бизнесмену с кейсом денег както не очень. Можно, конечно, снять отдельную комнату и закрыться там, но коридоры остаются общие с другими посетителями. И никто не даст гарантию, что в соседней комнате не устроят пожара или не будут кричать всю ночь под окнами. Да и ключи все еще есть у администратора. Еще один вариант – арендовать или выкупить весь хостел целиком. Что уже неплохо, но ряд проблем все равно придется решать. В этом примере легко просматриваются отсылки к разным типам (SaaS, PaaS, IaaS) облачных сервисов, а также частным и публичным облакам.

Еще один пример. В облаках мы не можем осуществлять самостоятельный контроль за сохранностью данных и должны передать эти полномочия другим людям. Напрашивается аналогия с банковскими депозитами. Мы можем сложить деньги под подушку или в чемоданчик с ключом – и при этом постоянно беспокоиться за них. Или же отдать на хранение в учреждение, предоставляющее гарантии сохранности денег, –

банк. Беспокоиться все равно будем, но безопасность наших сбережений в таком случае обеспечивается репутацией организации и государственными гарантиями, такими как Система страхования вкладов и регламенты СТО БР. Посмотрите вокруг, банки вошли в нашу жизнь, и их услугами пользуются все. Можно ожидать подобного и в области хранения и обработки информации. С течением времени операторы ЦОД выйдут на высокий уровень защищенности, заработают репутацию, а государственные органы выработают стандарты защиты (начало положено указами ФСТЭК по защите виртуализации, а также готовящимися к выходу ГОСТами по защите в облаках и по защите виртуализации). Возможно, хранить свои данные в облаке станет безопаснее, чем локально.

Несколько советов

Вернемся к периметру, а точнее, к той динамической структуре, в которую он превратился. Понятно, что в такой схеме невозможно осуществлять полный самостоятельный контроль своих постоянно меняющихся границ и приходится доверять внешнему управляющему, гипервизору, на которого ложится гигантская ответственность. И в целом нельзя сказать, что гипервизоры не готовы к ней. Да, периодически находятся новые уязвимости, но надо понимать, что уязвимости есть в абсолютно любой системе. Мы научились доверять автопилотам и бортовым системам в самолете свои жизни, нам придется научиться доверять гипервизорам свои данные.

Но это не значит, что мы ни на что не можем повлиять. Есть несколько общих моментов, которые необходимо учитывать.

Во-первых, не стоит впадать в паралич перфекциониста. "Если я не могу быть уверен, что данные из ОЗУ моей виртуальной машины не попадут в другую виртуальную машину, то они де-факто скомпрометированы и можно даже не пытаться их спасти", – в корне неправильная позиция. В ней нарушается один замечательный принцип: "убегая от медведя, не нужно бежать быстрее всех, важно бежать быстрее последнего". Следует всегда помнить, что многие атаки, хоть и возможны в теории, но на практике чрезвычайно сложны и могут потребовать серьезных ресурсов и высочайшей квалификации исполнителя. Никто в жизни не попытается атаковать гипервизор крупного хостинга ради ваших данных, если их можно получить через тривиальную SQL-инъекцию на вашем сайте. Поэтому закройте потенциальные уязвимости адекватно стоимости своих данных. Естественно, что чем больше стоят данные, тем более надежную и контролируемую инфраструктуру придется выбрать. Да, не секрет, что построение собственного частного облака может оказаться дороже использования своего существующего публичного аналога. Но во все времена более высокий уровень защиты приводил к большим затратам.

Во-вторых, помогите защитить свои данные гипервизору тем, чем можете. Закройте часть входов в периметр самостоятельно. Шифруйте данные, записываемые на диск. Это снизит риск их компрометации. Шифруйте данные, выходящие через сетевые интерфейсы ваших устройств. Это чрезвычайно важно: огромный набор различных сетевых атак вам больше не страшен. Обеспечьте защищенный доступ к своим данным извне. На рынке сейчас существует ряд продуктов по шифрованию и межсетевому экранированию, в том числе в виртуализированных средах. Надо сказать, что если раньше подобная защита была доступна только у западных вендоров, то сейчас появились и отечественные разработки, полностью отвечающие требованиям регулятора в области защиты персональных данных.

Резюмируя все вышесказанное

Еще раз обратим внимание: периметр – не исчез. Но он трансформировался в более сложную сущность, которую человек не в силах контролировать напрямую в реальном времени, и в вопросах его защиты приходится полагаться на соответствующие инструменты. В этом нет ничего страшного, но поскольку на данном этапе данные инструменты находятся в начале своего долгого пути, следует не забывать и о традиционных методах защиты, которые не менее важны. ●

Комментарий эксперта

Антон Шкарин,
руководитель группы разработки продукта "Гарда Предприятие", компания "МФИ Софт"

Как защитить DLP-систему от атак?

Большинство современных DLP-систем построены на основе клиент-серверной архитектуры. Как правило, хранение и обработка информации (в том числе и конфиденциальных данных) осуществляется именно на сервере. Клиент же представляет собой "тонкое" приложение с логикой, ограниченной обменом информацией с сервером и визуализацией полученных от сервера данных.

Поэтому и защиту DLP-системы можно разделить на несколько уровней:

1. Защита сервера;
2. Защита клиента;
3. Защита канала между сервером и клиентом.

Хорошим подходом к обеспечению безопасности сервера является, в первую очередь, изоляция его от внешнего мира, в том числе, от прямого доступа из Интернета (сервер находится в отдельной локальной подсети). Эта достаточно просто реализуемая мера сильно осложнит проведение атак на сервер DLP-системы хакерами. Далее следует позаботиться об организации хранения данных на сервере. Если доступ к ней был все-таки получен, шифрация данных на жестких дисках или своя файловая система делают трудозатраты по приведению такой информации к читаемому виду (по сути, декодированию) настолько большими, что сроки и стоимость выполнения такой работы могут превышать сроки актуальности самой информации, хранящейся на сервере DLP.

Защита клиента сводится к реализации системы управления доступом и разграничения прав (дискреционная, ролевая или мандатная модель), включающей в себя аутентификацию пользователей (вход по логину/паролю + дополнительные ограничения на сложность пароля, время его жизни, количество неверно введенных пар логин-пароль и прочие механизмы). В дополнение к этому действия каждого оператора DLP-системы необходимо логировать, чтобы защитить систему от одного из худших случаев, когда оператор является нарушителем информационной безопасности. Данное средство позволит руководителю отдела ИБ (или сотруднику, на которого возложены такие обязанности) выявлять недобросовестных пользователей DLP-системы.

Для обеспечения защиты канала связи между сервером и клиентом стандартом де-факто стало использование криптографических протоколов SSL или TLS, которые предотвращают возможность прослушивания канала.

Совокупность вышеописанных мер делает DLP-систему хорошо защищенной от хакерских атак и недобросовестных операторов. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru