но к примеру, такие задачи как создание, назначение VLAN, производится в ручную, проводя конфигурацию на каждом сетевом устройстве обособленно.

Еще один минус современных традиционных сетей, это нехватка гибкости в определении передачи данных. Коммутаторы устанавливают адресацию по MAC адресам, маршрутизаторы по IP адресам. Большинство специализированных сетевых устройств принимают решение о передаче данных в зависимости от содержания высылаемого пакета. Для определения пути можно использовать протокол PBR (PolicyBasedRouting), но для этого надо использовать ACL. ACL конфигурация на уровне управления, а не на уровне контроля, что ограничивает динамику в принятии решения.

Технология централизации систем управления в сетях используется достаточно давно. Это и системы телефонии, и ATM, и RADIUS, и контроллеры WiFi.

История развития централизованного управления сетью и развитие SDN сети начинается с ForCES (ForwardingandControlElementSeparation) 2003г. Инициатива IETF отделить управление сетью от передачи пакетов. 4D-Clean Slate 2005г. был задан вопрос: “Какой была-бы компьютерная сеть если создавать заново?” OpenFlow 2008г. Первая SDN спецификация.

Концепция сетей SDN основательно меняет принципы функционирования сетей и их управления. Один из важнейших принципов сетей SDN миграция уровня контроля из сетевых устройств и передача контроллеру. Контроллер SDN управляет всеми коммутаторами в сети и программирует каждый из них для правильной передачи трафика. Централизация логики управления позволяет программировать сеть как единое целое и упростить операционную модель больших корпоративных сетей, которые слишком статичны на данный момент.

Система SDN состоит из:

- Сетевые устройства. Их задача реализация заданий назначиных контроллером.
  - Програмное обеспечение, а именно программные сетевые устройства с возможностью реализовать протокол OpenFlow. Такие устройства медленнее, но имеют меньше ограничений что касаетсся памяти и функциональности. К примеру Nicira Open vSwitch и Big Switch Indigo.
  - Технические устройства. Это сетевые устройства предназначенные для обработки большого потока данных. Эти устройства используют такие технические элементы как CAM, TCAM, ASIC.
- Контроллер.
- Приложения. Приложения являются основой системы (не контроллер). Некоторые приложения могут быть представлены как составляющие контроллера. Приложения с помощью контроллера направляют команды для коммутаторов.

Кроме растущей популярности, сети SDN получает не мало критики. Часто критика поступает от производителей сетевого оборудования. Организовывая сеть SDN нужно обратить внимание на то, где будет находится контроллер, как будет организован мониторинг контроллера.

Например протоколы FTP, H323 и др. во время сессии меняют номера портов. В OpenFlow стандарте не указан контроль за содержанием пакета, поэтому заметить динамики изменения портов невозможно.

Н.Л.БОБРОВА[1]

АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ SECURITY AS A SERVICE

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» г. Минск, Республика Беларусь*

Причина популярности облачных вычислений связана с тем, что они призваны обеспечивать сбережение ресурсов и экономию средств. Перемещая в облако программное обеспечение, ресурсы хранения, электронную почту и т. д., организации получают возможность выделять ресурсы лишь в том объеме, который необходим для соответствующих сервисов. Пространство систем хранения, вычислительная мощность, память и даже лицензии больше не находятся в пассивном ожидании операций, которые они могли бы выполнить. Эти ресурсы используются и оплачиваются по мере возникновения необходимости. Такие технологии уже не только

применяются в мировых сферах бизнеса, но и пользуются большой популярностью в нашей стране. Облачные вычисления (англ. cloud computing) — информационно-технологическая концепция, подразумевающая обеспечение повсеместного и удобного сетевого доступа по требованию к общему пулу (англ.pool) конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам — как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами или обращениями к провайдеру. Потребители облачных вычислений могут значительно уменьшить расходы на инфраструктуру информационных технологий (в краткосрочном и среднесрочном планах) и гибко реагировать на изменения вычислительных потребностей, используя свойства вычислительной эластичности (англ.elastic computing) облачных услуг [1].

Облачные вычисления породили такое явление как SaaS (Software as a Service) – бизнес-модель продажи и использования ПО, когда поставщик разрабатывает приложение и сам управляет им, предоставляя заказчику доступ к ПО через сеть Интернет. Среди облачных сервисов SaaS-услуги пользуются наибольшим спросом у белорусских пользователей. Однако существует проблема безопасности и надежности услуг. На данный момент у потребителей достаточно большой выбор различных сервисов, в числе которых можно выделить «Безопасность как сервис» (SECaaS, Security As A Service) – это бизнес-модель, построенная таким образом, что крупный сервис-провайдер предоставляет интеграцию всех имеющихся сервисов безопасности в единую корпоративную инфраструктуру, что экономически более выгодно и эффективно, нежели большинство индивидуальных фирм или корпораций предоставят их самостоятельно с учетом совокупной стоимости данных сервисов [2]. SECaaS занимается переводом на аутсорсинг провайдеру возникающих проблем (антивирусы, спам-фильтры и т. п.) или же передачу в частное облако самой компании, но кроме всего этого SECaaS обозначает контроль безопасности предприятия, который осуществляет сторонняя организация. Использование облачных вычислений будет не только более полезным, но и куда более гибким: уходит необходимость каждый год приобретать лицензионное ПО, оплата идет прямо пропорционально реальному объему использования ПО (метод подписки на сервис). Кроме того отсутствует «привязка» клиента к конкретному производителю, поскольку используется централизованное управление решениями от разных производителей.

Преимуществами SECaaS являются:

– стабильные обновления вирусных баз, которые не зависят от грамотности пользователя;

– уровень безопасности экспертизы гораздо выше, чем у обычно существующей экспертизы в рамках конкретной организации;

– более быстрая управляемость учетными записями пользователей;

– аутсорсинг административных задач (например, таких, как управление журналом) позволяет снизить расходы времени и материальных ресурсов компании, а также предоставляет возможность уделять больше времени ее основной компетенции;

– веб-интерфейс на одинаково высоком уровне используется в администрировании конкретных задач и текущей деятельности [5].

Пользователь не устанавливает никакого стороннего программного обеспечения, поскольку это все оформляется в виде подписки на обновления пополняющихся «черных» списков вредоносных URL и IP, сигнатур спама.

К сервисам, что предоставляет SECaaS относят следующее:

– антиспам-защита;
– антивирусная защита;
– защита от атак типа «отказ в обслуживании» (DoS/DDoS);
– оценка безопасности;
– защита мобильных устройств (поддержка IOS / Android);
– управление, обнаружение и предотвращение вторжений;
– шифрование данных;
– восстановление после катастроф (предотвращение потери данных);
– управление событиями информационной безопасности;
– управление учетными записями и доступом;
– предотвращение утечек данных (DLP) [6].

Одним из самых важных сервисов является антивирусная защита. Кардинально новых решений нет. Когда клиент покупает нужное ему ПО, то больше оплачивает подписку, что дает возможность получать постоянно обновляемые сигнатуры, без чего антивирус становится куда менее полезным (он может отлавливать известные вирусы лишь на определенный момент, не получая информации о новых). В SECaaS же обработка файла ведется на облачном антивирусе (отсылается только часть файла, контрольная сумма, что сокращает нагрузку на сеть). Таким образом, спектр услуг, который можно отдать на аутсорсинг, достаточно велик. Например, журналирование занимает много времени и требует наличие инженера по обеспечению безопасности в штате но, будет проще и дешевле оплатить подписку на SECaaS. Однако, несмотря на прогресс в развитии информационных технологий и услуг информационной безопасности, многие просто не готовы отдать этот элемент бизнеса на аутсорсинг. Причины:

– клиенты боятся потерять свои данные, поскольку безопасность будет передана сторонней организации;

– отсутствие стандартов.

Но технология развивается. SECaaS используют такие предприятия, как Cisco, McAfee, Panda Software, Symantec, Trend Micro и VeriSign [7].

С продвижением облачных технологий и увеличения числа облачных пользователей, размеры безопасности данных будут постоянно увеличиваться, что будет требовать улучшения аспектов защиты информации. Ответственность за будущее всех облачных сервисов (в том числе и SECaaS) лежит на поставщиках. Поэтому их первоочередная задача – завоевание доверия клиентов и повышение качества поставляемых услуг. SECaaS представляет собой удобный, многофункциональный элемент для управления безопасностью предприятия, что во многом позволяет экономить на информационной безопасности. Простой в обращении, надежный, экономичный сервис завоевывает всю большую аудиторию, демонстрируя универсальность «облака».

ЛИТЕРАТУРА

1. Безкоровайный, Д. Security as a Service. Что должен уметь провайдер [Электронный ресурс] – Режим доступа : URL:http://www.iksmedia.ru/articles/3928552-Security-as-a-Service-Chto-dolzh... – Дата доступа : 27.04.2016.

2. Облачные сервисы[Электронный ресурс] – Режим доступа : URL:http://www.tadviser.ru/index.php/Статья:Облачные_сервисы – Дата доступа : 28.03.2016.

3. Первая на российском рынке облачная услуга информационной безопасности [Электронный ресурс] – Режим доступа : URL:http://www.croc.ru/news/detail/41733/ – Дата доступа : 29.05.2016.

4. Понятие облачных технологий [Электронный ресурс] – Режим доступа. – URL:http://technologies.hut4.ru/onecol.html - Дата доступа: 5.06.2016.

5. CYREN – безопасность как сервис (SECaaS) для защиты от интернет угроз [Электронный ресурс] – Режим доступа : URL:http://certsys.ru/events/?events=438 – Дата доступа : 22.04.2016.

6. SaaS [Электронный ресурс] – Режим доступа : URL:http://www.tadviser.ru/index.php/Статья:SaaS – Дата доступа : 29.04.2016.

7. What is security-as-a-service (SECaaS)? [Электронный ресурс] – Режим доступа : URL:http://searchsecurity.techtarget.com/definition/Security-as-a-Service) – Дата доступа : 29.05.2016.

А.В.МИНИЧ[1]

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ METEUM ДЛЯ ТОЧНОГО РАСЧЕТА ПРОГНОЗА ПОГОДЫ

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

В наше время метеорологические прогнозы занимают важную роль как в жизни отдельных людей, так и целой страны. В развитых странах погода и климат давно стали категориями экономическими. Особенно заметный экономический эффект дает использование метеорологической информации в авиации, энергетике, строительстве, рыболовстве и